



BULLETIN (SB26-187)
VULNERABILITY SUMMARY FOR THE WEEK OF
29TH JUNE, 2026



Bulletin (SB26-187) Vulnerability Summary for the Week of June 29, 2026

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by the division of high, medium and low severities correspond to the following scores:

High- Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0.

Medium - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0.6.9 -

Low - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9.

Entries may include additional information provided by organizations and efforts sponsored by Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis .

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cline--cline	Cline is an autonomous coding agent as an SDK, IDE extension, or CLI assistant. In versions 2.13.0 and prior, there is a cross-origin WebSocket hijack vulnerability in Cline Kanban servers. At time of publication, there are no publicly available patches.	2026-06-01	9.6	CVE-2026-44211
Cloud Foundry Foundation--BOSH	PackagePersister.validate_tgz builds "tar -tf #{tgz} 2>&1" where tgz = File.join(release_dir, 'packages', "#{name}.tgz") and name = package_meta['name'] comes directly from release.MF inside the uploaded tarball. The string is passed to Bosh::Common::Exec.sh, which executes via %x{} - i.e., /bin/sh -c. No Shellwords.escape is applied. The Models::Package Sequel validation (VALID_ID = /^[0-9A-Za-z_+]+\$/i) would reject the name, but in create_package (lines 74-79) the shell-out in save_package_source_blob runs before package.save, so validation fires too late. Affected versions: - BOSH: all versions prior to v282.1.12 (inclusive); fixed in v282.1.12 or later	2026-06-04	8.2	CVE-2026-41011
Cloud Foundry Foundation--BOSH	CWE-326 in BOSH allows a local attacker to steal Basic-auth credentials or redirect UAA token requests via MITM. HttpRequestHelper#create_async_endpoint and #send_http_get_request_synchronous hard-code OpenSSL::SSL::VERIFY_NONE, enabling an attacker to intercept traffic between bosh-monitor and the BOSH director or UAA and steal credentials. Affected versions: - BOSH: all versions prior to v282.1.9 (inclusive); fixed in v282.1.9 or later	2026-06-04	8.8	CVE-2026-41860
Cloud Foundry Foundation--BOSH	A network man-in-the-middle between nats-sync and the BOSH director can steal the director credentials (Basic auth header or UAA client secret) and can tamper with the VM list that is written into the NATS authorization file. Stolen credentials grant administrative director access. UsersSync#bosh_api_response_body builds a Net::HTTP client with verify_mode = OpenSSL::SSL::VERIFY_NONE for every director call (/info, /deployments, /deployments/<name>/vms). Affected versions: - BOSH: all versions prior to v282.1.9 (inclusive); fixed in v282.1.9 or later	2026-06-04	7.8	CVE-2026-41859
Cloud Foundry Foundation--BOSH Director	ReleaseJob#unpack builds job_dir = File.join(@release_dir, 'jobs', name) and job_tgz = File.join(@release_dir, 'jobs', "#{name}.tgz") where name returns @job_meta['name'], a value taken verbatim from the jobs: array of the attacker-supplied release.MF inside the uploaded tarball. These paths are then interpolated into a shell string: Bosh::Common::Exec.sh("tar -C #{job_dir} -xf #{job_tgz} 2>&1", :on_error => :return). Bosh::Common::Exec.sh executes via %x#{command} (bosh-common/lib/bosh/common/exec.rb:53), i.e. /bin/sh -c, so any shell metacharacters in name are interpreted. FileUtils.mkdir_p(job_dir) on line 49 creates the literal directory (no shell) and succeeds even when the name contains \$()/,; so execution reaches the sh call. Affected versions: - BOSH Director: all versions prior to v282.1.12 (inclusive); fixed in v282.1.12 or later	2026-06-04	8.2	CVE-2026-41010
Cloud Foundry Foundation--log-cache_release	Authentication Bypass in cf-auth-proxy in Cloud Foundry Foundation all installations allows an unauthenticated remote attacker to gain read access to every log and metric for every application and platform component via minting a JWT that the cf-auth-proxy accepts as a valid logs.admin token. Affected versions: - log-cache_release: all versions through v3.2.6 (inclusive); fixed in v3.2.7 or later - CF Deployment: all versions through v55.?0 (inclusive); fixed in v55.?0 or later (bundles log-cache_release v3.2.7)	2026-06-01	7.5	CVE-2026-40964
Cloud Foundry Foundation--uaa_release	Cloud Foundry UAA versions v76.12.0 through v78.12.0 are vulnerable to a private key exposure. The server contains a vulnerability where EC (Elliptic Curve) private keys are inadvertently exposed through the public /token_keys endpoint. This endpoint is designed to provide public key material for JWT token verification but incorrectly exposes private key components for EC keys. The vulnerability affects deployments using EC keys for JWT token signing. The vulnerability does not affect RSA key configurations, only deployments using EC keys for JWT signing. Affected	2026-06-01	10	CVE-2026-40965

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	versions: - uaa_release: v76.12.0 through v78.12.0 (inclusive); fixed in v78.13.0 or later - CF Deployment: v30.0.0 through v56.0.0 (inclusive); fixed in v56.1.0 or later (bundles uaa_release v78.13.0)			
CloudburstMC--Network	Cloudburst Network provides network components used within Cloudburst projects. A vulnerability in versions prior to `1.0.0.CR3-20260417.085727-30` impacts publicly accessible software depending on the affected versions of Network and allows an attacker to exploit a vulnerability in Network to stall the netty event loop, rendering it inoperable. All consumers of the library should upgrade to at least version `1.0.0.CR3-20260417.085727-30`. There are no known workarounds beyond updating the library.	2026-06-05	7.5	CVE-2026-45290
CloudburstMC--Network	Cloudburst Network provides network components used within Cloudburst projects. A vulnerability in versions prior to `1.0.0.CR3-20260418.124334-32` impacts publicly accessible software depending on the affected versions of Network and allows an attacker to exploit a bug in Network to close the parent netty channel, rendering it inoperable. All consumers of the library should upgrade to at least version `1.0.0.CR3-20260418.124334-32`. There are no known workarounds beyond updating the library.	2026-06-05	7.5	CVE-2026-45291
CloudPirates-io--helm-charts	CloudPirates Open Source Helm Charts is a collection of Helm charts. Prior to commit fcf9302, a GitHub Actions workflow (pull-request.yaml) executes attacker-controlled code from fork pull requests in a privileged context, exposing repository secrets including Docker Hub credentials and tokens without requiring maintainer approval. This issue has been patched via commit fcf9302.	2026-06-01	10	CVE-2026-45131
CloudPirates-io--helm-charts	CloudPirates Open Source Helm Charts is a collection of Helm charts. Prior to commit fcf9302, a GitHub Actions workflow (generate-schema.yaml) exposes sensitive credentials (Personal Access Token and SSH signing key) to fork-controlled code due to unsafe checkout and credential handling practices. This issue has been patched via commit fcf9302.	2026-06-01	10	CVE-2026-45132
Code Supply Co.-Blueprint	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Code Supply Co. Blueprint allows PHP Local File Inclusion. This issue affects Blueprint: from n/a before 1.1.5.	2026-06-02	8.1	CVE-2026-39552
code-projects--Hotel and Tourism Reservation System	A vulnerability was identified in code-projects Hotel and Tourism Reservation System 1.0. This issue affects the function password_verify of the file /admin/login.php of the component Admin Login. Such manipulation of the argument Password leads to improper authentication. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	2026-06-01	7.3	CVE-2026-10288
code-projects--Hotel and Tourism Reservation System	A weakness has been identified in code-projects Hotel and Tourism Reservation System 1.0. The affected element is an unknown function of the file tour.php of the component GET Parameter Handler. Executing a manipulation of the argument tour can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.	2026-06-01	7.3	CVE-2026-10290
code-projects--Hotel and Tourism Reservation System	A vulnerability has been found in code-projects Hotel and Tourism Reservation System 1.0. This affects an unknown function of the file /details.php. Such manipulation of the argument room leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2026-06-05	7.3	CVE-2026-11342
code-projects--Online Hospital Management System	A flaw has been found in code-projects Online Hospital Management System 1.php. This impacts the function login_user of the file login_1.php. Executing a manipulation of the argument Username can lead to sql injection. The attack can be executed remotely. The exploit has been published and may be used.	2026-06-01	7.3	CVE-2026-10208
code-projects--Real State Services	A vulnerability has been found in code-projects Real State Services 1.0. This impacts an unknown function of the file /loginuser.php of the component Login. The manipulation of the argument Username leads to	2026-06-01	7.3	CVE-2026-10262

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.			
code-projects--Smart Parking System	A security vulnerability has been detected in code-projects Smart Parking System 1.0. Affected is an unknown function of the component Admin Endpoint. Such manipulation leads to missing authentication. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. Multiple endpoints are affected.	2026-06-01	7.3	CVE-2026-10243
code-projects--Student Admission System	A flaw has been found in code-projects Student Admission System 1.0. Affected is an unknown function of the file /index.php. This manipulation of the argument eid/did causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used.	2026-06-02	7.3	CVE-2026-10620
code-projects--Vehicle Management System	A vulnerability was found in code-projects Vehicle Management System 1.0. This impacts an unknown function of the file newdriver.php of the component New Driver Registration Form. Performing a manipulation of the argument photo results in unrestricted upload. The attack may be initiated remotely. The exploit has been made public and could be used.	2026-06-05	7.3	CVE-2026-11344
CodeAstro--Online Job Portal	A vulnerability was detected in CodeAstro Online Job Portal 1.0. The impacted element is an unknown function of the file /admin/jobs-admins/delete-jobs.php. Performing a manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	2026-06-01	7.3	CVE-2026-10260
CodeAstro--Online Job Portal	A flaw has been found in CodeAstro Online Job Portal 1.0. This affects an unknown function of the file /users/application_status.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	2026-06-01	7.3	CVE-2026-10261
codepress--Admin Columns	The Admin Columns plugin for WordPress is vulnerable to PHP Object Injection leading to Remote Code Execution in versions up to and including 7.0.18. This is due to the use of `unserialize()` without an `allowed_classes` restriction in the `IdsToCollection::get_ids_from_string()` function, which processes attacker-controlled post meta values without proper validation. This makes it possible for authenticated attackers with Contributor-level access and above to inject a serialized PHP object into a post's custom meta field and trigger arbitrary code execution by exploiting a bundled POP gadget chain, resulting in remote code execution as the web server user.	2026-06-05	8.8	CVE-2026-7654
Comodo--Comodo Internet Security	Comodo Internet Security's firewall driver Inspect.sys contains an integer underflow in its IPv6 packet parser. The parser decrements an unsigned 64-bit payload-length value (taken from the IPv6 fixed header's payload length field) by the size of each IPv6 extension header without validating it, so a packet whose declared payload length is smaller than the sum of its extension-header lengths underflows the value to a near-maximal 64-bit integer. Because IPv6 parsing occurs before firewall rule enforcement, a remote, unauthenticated attacker can send a single crafted IPv6 packet - even to a host with all ports blocked - to trigger an out-of-bounds read (and, on a separate code path, an oversized memcpy) in the Windows kernel at DISPATCH_LEVEL, crashing the system (BSOD).	2026-06-07	7.5	CVE-2026-49494
coreshop--CoreShop	CoreShop is a Pimcore enhanced eCommerce solution. In versions 5.0.1 through 5.1.0-beta.1,, the GitHub Actions workflow (`.github/workflows/static.yml`) uses the `pull_request_target` trigger but dangerously checks out the unverified code from the pull request head (`ref: \${github.event.pull_request.head.ref}`). Subsequently, it executes a script (`.bin/console`) from this untrusted checkout. This allows any external attacker to achieve Remote Code Execution (RCE) on the GitHub Actions runner simply by submitting a malicious Pull Request. Also known as a "Pwn Request" vulnerability. As of time of publication, `pull_request_target` is still in the file.	2026-06-04	8.2	CVE-2026-41249
crmeb--crmeb_java	A vulnerability was found in crmeb crmeb_java 1.4. Affected is the function RestTemplate.getForEntity of the file crmeb-	2026-06-03	7.3	CVE-2026-10771

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	common/src/main/java/com/zbkj/common/utis/RestTemplateUtil.java of the component base64 Qrcode Endpoint. The manipulation of the argument url results in server-side request forgery. The attack can be executed remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.			
D-Link--DI-8400	A vulnerability was detected in D-Link DI-8400 up to 16.07.26A1. This affects an unknown function of the file /dbsrv.asp. Performing a manipulation of the argument str results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used. The initial researcher advisory mentions contradicting parameter names to be affected.	2026-06-01	8.8	CVE-2026-10206
danny-avila--LibreChat	LibreChat is an enhanced ChatGPT clone that supports multiple AI providers. In versions up to and including 0.8.3, the Model Context Protocol (MCP) server integration resolves \${VAR} placeholders against the server's process.env during Zod schema validation of user-supplied MCP server URLs. Any authenticated user can create a malicious MCP server configuration with a URL pointing to an attacker-controlled domain containing environment variable references, causing the LibreChat server to connect to the attacker's server and transmit critical secrets such as CREDNS_KEY, CREDNS_IV, JWT_SECRET, and MONGO_URI in the request URL. This enables full compromise of the installation's cryptographic materials and database credentials without requiring administrative privileges. This is patched in version 0.8.4-rc1.	2026-06-02	9.6	CVE-2026-32625
danny-avila--LibreChat	LibreChat is an enhanced ChatGPT clone that supports multiple AI providers. In versions up to and including 0.7.6, an Insecure Direct Object Reference (IDOR) vulnerability exists in the API keys management endpoint (PUT /api/keys). Due to the use of the JavaScript object spread operator after setting the authenticated user's ID, any authenticated user can inject a userId parameter in the request body to overwrite any other user's API keys (e.g., OpenAI, Anthropic, Azure). This allows an attacker to replace a victim's API key configuration, potentially routing the victim's conversations through attacker-controlled keys or denying service by providing invalid keys. This is patched in version 0.8.3-rc1.	2026-06-02	7.1	CVE-2026-31942
Dassault Systmes--DELMIA Service Process Engineer	A Stored Cross-site Scripting (XSS) vulnerability affecting Process Experience Studio in DELMIA Service Process Engineer from Release 3DEXPERIENCE R2024x through Release 3DEXPERIENCE R2026x could allow an attacker to execute arbitrary script code in user's browser session.	2026-06-01	8.7	CVE-2026-9024
Dassault Systmes--Teamwork Cloud - Standard Edition	A Deserialization of Untrusted Data vulnerability affecting Teamwork Cloud from No Magic Release 2022x through No Magic Release 2026x and Magic Collaboration Studio from CATIA Magic Release 2022x through CATIA Magic Release 2026x could lead to an unauthenticated remote code execution.	2026-06-01	9.8	CVE-2026-7858
DatanoiseTV--tinyice	TinyIce is a streaming server for audio and video. In versions 0.8.95 through 2.4.1, missing authentication on WebRTC ingest endpoint allows unauthenticated stream injection. Version 2.5.0 fixes the issue by requiring either HTTP Basic auth or a `?password=` query parameter, comparing the supplied password against the per-mount source password (or the `default_source_password` fallback) using bcrypt, hooking into the existing brute-force IP rate-limiter (5 failed attempts per IP within 15 minutes triggers a lockout), and rejecting requests for mounts in `disabled_mounts`. The same release also tightens an adjacent endpoint, `POST /admin/golive/chunk`, which previously required session authentication but did not verify the session user's per-mount access nor check the CSRF token.	2026-06-05	8.2	CVE-2026-45327
davidanderson--All-In-One Security (AIOS)	The All-In-One Security (AIOS) - Security and Firewall plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to and including 5.4.7. This is due to insufficient input sanitization in the get_rest_route()	2026-06-06	7.2	CVE-2026-8438

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Security and Firewall	function and missing output escaping in the column_default() method of the debug log list table. When the 'Disable REST API for non-logged in users' feature (aiowps_disallow_unauthorized_rest_requests) is enabled alongside debug logging (aiowps_enable_debug), an unauthenticated attacker can embed arbitrary HTML or JavaScript in the REST request path. The path is retrieved via urldecode(\$_SERVER['REQUEST_URI']), which decodes URL-encoded payloads into literal HTML characters. This decoded, unsanitized value is concatenated directly into a debug log message and stored in the database. When an administrator navigates to the AIOS Dashboard Debug Logs page, the column_default() method returns the raw database value without escaping, and the parent list table echoes it directly, causing JavaScript execution in the administrator's browser session. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute when an administrator views the debug log page, enabling nonce theft, privileged AJAX/REST actions, and potential full site compromise.			
DedeCMS--DedeCMS	A vulnerability was determined in DedeCMS 5.7.88. The affected element is the function TrimMsg of the file /plus/feedback.php of the component Feedback Handler. Executing a manipulation of the argument msg can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	2026-06-02	7.3	CVE-2026-10606
DedeCMS--DedeCMS	A vulnerability was identified in DedeCMS 5.7.88. The impacted element is the function dede_htmlspecialchars of the file /plus/flink.php. The manipulation of the argument msg leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	2026-06-02	7.3	CVE-2026-10607
DedeCMS--DedeCMS	A security flaw has been discovered in DedeCMS 5.7.88. This affects the function RemoveXSS of the file /plus/carbuyaction.php. The manipulation of the argument postname/des results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-06-02	7.3	CVE-2026-10608
defenseunicorns--uds-identity-config	UDS Identity Config builds the Keycloak configuration image (realm, plugins, theme, truststore, JARs) consumed by UDS Core's Identity deployment. In versions 0.11.0 through 0.26.0, a logic error in the `client-kubernetes-secret` Keycloak client authenticator (shipped by `uds-identity-config` and consumed by UDS Core) causes the submitted `client_secret` to be overwritten with the mounted Kubernetes secret before comparison. An attacker who can reach the Keycloak token endpoint and knows a `client_id` using this authenticator can authenticate as that client with any `client_secret` value and obtain OAuth2 tokens scoped to the client's service account. In the case of the `uds-operator` client this token can be used to registry/modify other clients. Version 0.26.1 patches the issue.	2026-06-05	10	CVE-2026-46389
Dell--BSAFE SSL-J	Dell BSAFE SSL-J contains an allocation of resources without limits or throttling vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to a Denial of Service (DoS).	2026-06-04	7.5	CVE-2025-46638
Dell--ThinOS 10	Dell ThinOS 10, versions prior to ThinOS10 2602_10.0765, contain an Improper Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Privilege Escalation.	2026-06-02	7.8	CVE-2026-40715
Dräger--CC-Vision Basic	Dräger CC-Vision Basic before 7.5.3 and Dräger CC-Vision E-Cal before 7.2.5.0 contain an out-of-bounds write vulnerability when loading .gdt files. A crafted .gdt file can trigger a buffer overflow during file parsing, allowing an attacker to crash the application or execute malicious code on the underlying system.	2026-06-02	8.2	CVE-2021-4478
Dräger--Core	Dräger Core 1.0.5 and Dräger M540 Converter Service 1.0.9 contain a denial of service vulnerability that allows network-adjacent attackers to trigger high CPU load by sending specially crafted, unencrypted SDC messages during the discovery process. Attackers with access to the hospital network can send malformed SDC packets to exhaust CPU	2026-06-02	7.5	CVE-2024-14036

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	resources in the affected process, causing further SDC messages to no longer be processed.			
Dräger--Infinity Acute Care System	Dräger Infinity Acute Care System and Standalone Infinity M540 patient monitors running software versions VG4.1.1, VG4.0.3, and lower contain network message handling vulnerabilities that allow network-adjacent attackers to spoof or tamper with data and cause denial-of-service conditions. Attackers with access to an enabled Infinity network port or physical proximity to a wireless access point can modify device settings such as alarm states or alarm limits, and overwhelm the system with incoming data causing the device to reboot and lose network functionality.	2026-06-02	8.6	CVE-2019-25719
Dräger--Infinity Acute Care System	Dräger Infinity Acute Care System and Standalone Infinity M540 patient monitors versions VG4.1.1, VG4.0.3, and lower (with VG4.2 partially affected) contain a network message handling vulnerability that allows remote attackers to inject spoofed or tampered data and cause denial-of-service conditions. Attackers can compromise network communications to modify device settings such as alarm states or alarm limits, or overwhelm the system with excessive network traffic causing the Cockpit or M540 to reboot and lose network functionality.	2026-06-02	8.6	CVE-2022-4992
Dräger--Infinity Explorer C700	Dräger Infinity Explorer C700 contains a privilege escalation vulnerability that allows attackers to break out of kiosk mode and access the underlying operating system through a specific dialog interaction. Attackers can exploit this kiosk escape to take control of the operating system and cause the device to display incorrect or no information from the connected Delta Family patient monitor.	2026-06-01	8.4	CVE-2019-25718
Dräger--Protector Software	Dräger Protector Software prior to version 6.4.2 contains a local privilege escalation vulnerability due to insecure file system permissions that allows local attackers to execute arbitrary code with elevated privileges. Attackers can replace binaries or loaded modules on the host system to execute code with NT SYSTEM privileges.	2026-06-02	8.2	CVE-2021-4480
Dräger--Protector Software	Dräger Protector Software prior to version 6.4.2 contains a local privilege escalation vulnerability due to insecure file system permissions that allows local attackers to execute arbitrary code with elevated privileges. Attackers can replace binaries or loaded modules on the host system to execute code with NT SYSTEM privileges.	2026-06-02	8.2	CVE-2021-4481
Dräger--SC 6002XL	Dräger SC Monitoring devices (SC 6002XL, SC 6802XL, SC 7000, SC 8000, SC 9000 XL) contain hard-coded plaintext credentials in source code and a denial-of-service vulnerability that allows local and remote attackers to compromise device integrity across all software versions. A local attacker with direct device access can use the hard-coded credentials to access service and clinical accounts and alter device configuration, while a remote attacker can send malformed network packets to cause repeated device reboots, ultimately resulting in loss of network connectivity and disruption of patient monitoring.	2026-06-02	7.6	CVE-2019-25722
DTS Electronics Industry and Trade Ltd. Co.--Redline WR3200	Improper Authentication, Missing authentication for critical function, Weak Authentication vulnerability in DTS Electronics Industry and Trade Ltd. Co. Redline WR3200 allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Redline WR3200: from 7.1.3 before 7.1.8.	2026-06-05	9.8	CVE-2026-6274
E2Pdf.com--e2pdf	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in E2Pdf.Com e2pdf allows Reflected XSS. This issue affects e2pdf: from n/a through 1.32.14.	2026-06-01	7.1	CVE-2026-42681
e4jvikwp--VikBooking Hotel Booking Engine & PMS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in e4jvikwp VikBooking Hotel Booking Engine & PMS allows DOM-Based XSS. This issue affects VikBooking Hotel Booking Engine & PMS: from n/a through 1.8.8.	2026-06-01	7.1	CVE-2026-42683
ealpha072--Student-Management-System	A vulnerability was identified in ealpha072 Student-Management-System up to 01451bd7a2f58cdda07bd0b86e3967582e3ecd08. Affected by this issue is some unknown functionality of the file admin/config.php of the component Administrative Backend. Such manipulation leads to improper	2026-06-03	7.3	CVE-2026-10777

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authentication. The attack may be performed from remote. The exploit is publicly available and might be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.			
eitube--El-Tube	PHP El-Tube Script 3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the search parameter. Attackers can send GET requests to the search endpoint with crafted SQL payloads in the query parameter to extract sensitive database information including usernames, passwords, and version details.	2026-06-04	8.2	CVE-2019-25732
Elated-Themes--Aperitif	Deserialization of Untrusted Data vulnerability in Elated-Themes Aperitif allows Object Injection. This issue affects Aperitif: from n/a through 1.6.	2026-06-02	8.1	CVE-2026-39550
Elated-Themes--Askka	Deserialization of Untrusted Data vulnerability in Elated-Themes Askka allows Object Injection. This issue affects Askka: from n/a through 1.3.1.	2026-06-02	8.1	CVE-2026-39555
Elated-Themes--Tbel	Deserialization of Untrusted Data vulnerability in Elated-Themes TÃ¶bel allows Object Injection. This issue affects TÃ¶bel: from n/a through 1.8.1.	2026-06-02	8.1	CVE-2026-39551
eliekhoury--WP AutoSuggest	WP AutoSuggest 0.24 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the wpas_keys parameter. Attackers can send GET requests to autosuggest.php with crafted wpas_keys values to extract sensitive database information from WordPress posts and other tables.	2026-06-01	8.2	CVE-2018-25434
10Web--Photo Gallery by 10Web	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in 10Web Photo Gallery by 10Web allows Blind SQL Injection. This issue affects Photo Gallery by 10Web: from n/a through 1.8.41.	2026-06-04	7.6	CVE-2026-49771
AAM Plugin--Advanced Access Manager	Authentication Bypass by Spoofing vulnerability in AAM Plugin Advanced Access Manager allows URL Encoding. This issue affects Advanced Access Manager: from n/a through 7.1.0.	2026-06-01	7.5	CVE-2026-42674
ABB--T-MAC Plus	Files or directories accessible to external parties vulnerability in ABB T-MAC Plus. This issue affects T-MAC Plus: 4.0-24.	2026-06-03	9.9	CVE-2025-14771
ABB--T-MAC Plus	Authorization bypass through User-Controlled key vulnerability in ABB T-MAC Plus. This issue affects T-MAC Plus: 4.0-24.	2026-06-03	8.8	CVE-2025-14772
ABB--T-MAC Plus	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in ABB T-MAC Plus. This issue affects T-MAC Plus: 4.0-24.	2026-06-03	8	CVE-2025-14773
ABB--T-MAC Plus	Incorrect Authorization vulnerability in ABB T-MAC Plus. This issue affects T-MAC Plus: 4.0-24.	2026-06-03	7.4	CVE-2025-14774
ad-manager-wd--Ad Manager WD	WordPress Plugin ad manager wd 1.0.11 contains an arbitrary file download vulnerability that allows unauthenticated attackers to download sensitive files by manipulating the path parameter. Attackers can send GET requests to the edit.php endpoint with export=export_csv and a malicious path parameter to read arbitrary files like wp-config.php accessible to the web server.	2026-06-04	9.8	CVE-2019-25727
Ahmad--WP Job Portal	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Ahmad WP Job Portal allows Blind SQL Injection. This issue affects WP Job Portal: from n/a through 2.5.1.	2026-06-02	9.3	CVE-2026-42684
Ahmad--WP Job Portal	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ahmad WP Job Portal allows Reflected XSS. This issue affects WP Job Portal: from n/a through 2.5.1.	2026-06-02	7.1	CVE-2026-42685
Akmer Informatics Automation Industry and Trade Ltd. Co.--TeknoPass	Authorization bypass through User-Controlled SQL primary key vulnerability in Akmer Informatics Automation Industry and Trade Ltd. Co. TeknoPass allows SQL Injection. This issue affects TeknoPass: from 20210501 through 20260429.	2026-06-04	9.8	CVE-2026-4104
alfio-event--alf.io	alf.io is an open source ticket reservation system for conferences, trade shows, workshops, and meetups. Prior to version 2.0-M5-2606, a sandbox	2026-06-02	8	CVE-2026-35482

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	escape vulnerability in the alf.io extension script engine allows an authenticated administrator to execute arbitrary operating system commands on the server. The extension system is intended to execute restricted JavaScript in a sandboxed Rhino environment; however, a combination of an unguarded injected Java object (`returnClass`) and an incomplete AST blacklist allows the sandbox to be fully escaped using Java reflection without triggering any validation errors. Version 2.0-M5-2606 patches the issue.			
Allplayer--AllPlayer	AllPlayer 7.4 contains a local buffer overflow vulnerability in URL handling that allows attackers to overwrite structured exception handling pointers by supplying an excessively long URL string. Attackers can craft a malicious URL, paste it into the Open URL dialog, and trigger SEH-based code execution to run arbitrary commands with user privileges.	2026-06-04	8.4	CVE-2019-25735
androThemes--Cookiteer	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in androThemes Cookiteer allows PHP Local File Inclusion. This issue affects Cookiteer: from n/a through 1.4.8.	2026-06-02	8.1	CVE-2025-68886
Anionex--banana-slides	Banana Slides through 0.4.0, patched in commit e8bc490, contains a path traversal vulnerability in the generate_image() function within the AI service backend that allows unauthenticated attackers to read arbitrary image-format files outside the intended uploads directory by exploiting an incomplete path prefix check using os.path.startswith() without a trailing separator. Attackers can supply crafted markdown image references in user-controlled page descriptions that resolve to sibling directories whose names share the uploads folder prefix, bypassing the directory confinement check and causing the application to read files from unintended locations via PIL Image.open().	2026-06-01	7.5	CVE-2026-49136
Apache Software Foundation--Apache MINA	ZDRES-232: resolveProxyClass Not Overridden - acceptMatchers Filter Bypass via java.lang.reflect.Proxy Assessment: Fully addressed. When the serialised stream contains a TC_PROXYCLASSDESC (the marker for a java.lang.reflect.Proxy), JDK's ObjectInputStream.readProxyDesc() is dispatched. JDK then calls the default ObjectInputStream.resolveProxyClass(interfaces) implementation, which performs Class.forName(intf, false, latestUserDefinedLoader()) for EACH interface name and constructs the proxy class " bypassing the accepted classes list . ZDRES-233: Class.forName(name, initialize=true, classLoader) in readClassDescriptor Triggers Static Initialiser of Allow-Listed Classes Assessment: Fully addressed. For ANY class on the allow-list, deserialising a stream that names it triggers the class's (static initialiser) BEFORE any instance is constructed. This means an attacker who supplies a class name on the allow-list (e.g., the developer wrote accept("com.myapp.*") , attacker supplies com.myapp.SomeClass) causes <clinit> of SomeClass" and many real-world classes have side-effecting static initialisers Both issues have been fixed.	2026-06-03	9.8	CVE-2026-47065
Apache Software Foundation--Apache MINA SSHD	Path traversal vulnerability in Apache MINA SSHD bundle sshd-git. Lack of path validation in git-upload-pack, git-receive-pack, and other git operations allows users authenticated over SSH access to git repositories outside the configured git server root directory. Applications are affected if they use org.apache.sshd:sshd-git. Applications not using sshd-git are not affected. Users are advised to upgrade affected applications to Apache MINA SSHD 2.18.0, which fixes the issue. The issue also is present in the pre-release milestones 3.0.0-M1 to 3.0.0-M3 for a new upcoming new major version 3.0.0. Again, applications are affected only if they use sshd-git. Upgrade affected applications to 3.0.0-M4. We would like to point out that a professional git server should not rely solely on file system layout and permissions, but should implement additional security controls to govern access to git repositories and operations allowed on particular git repositories.	2026-06-01	7.1	CVE-2026-48827

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Apache Software Foundation-- Apache Solr	Hardcoded credentials in the Basic Authentication setup tool (bin/solr auth enable) in Apache Solr versions 9.4.0 through 9.10.1 and 10.0.0 allows a remote attacker to gain full administrative access to the cluster via publicly known default credentials installed silently alongside the user-specified account. As an immediate workaround without upgrading, delete the template users (superadmin, admin, search, index) from security.json or change their passwords. The future, not yet released, versions 9.11.0 and 10.1.0 will not be vulnerable, and it will be enough to upgrade to solve the issue. Not affected: * Clusters where bin/solr auth enable was not used to bootstrap BasicAuth * Clusters where template users have been assigned strong passwords after bootstrap	2026-06-01	8.1	CVE-2026-44825
Arista Networks--EOS	Affected platforms running Arista EOS with OpenConfig configured, a gNMI Set request can be run when it should have been rejected. This can result in unexpected configuration being applied to the switch.	2026-06-04	9.6	CVE-2024-27890
Arista Networks--EOS	Affected platforms running Arista EOS with OpenConfig configured, a gNMI Set request can be run when it should have been rejected. This can result in unexpected configuration being applied to the switch.	2026-06-04	9.6	CVE-2024-27892
Arista Networks--EOS	On affected platforms running Arista EOS with IPsec configured, a specially crafted packet can cause the dataplane to stop processing all IPsec traffic. The control plane may detect this condition, and attempt to reset the IPsec processing pipeline. After reset traffic may not resume being processed. There is no impact to non-IPsec traffic or to IPsec traffic not originating or terminating on the system. This issue was reported by an Arista customer.	2026-06-04	7.5	CVE-2025-8873
Arista Networks--EOS / CloudVision eXchange (CVX)	An authenticated Redis session could be used to obtain full root access to all servers in the CVX cluster. Note that this would require an attacker to have both network access to the Redis service on a CVX server and the Redis password. Please note that all Redis communication, including authentication, occurs over plaintext in the present day. TLS support is tracked under RFE1294850.	2026-06-05	8.3	CVE-2025-5088
Armcode--Arm Whois	Arm Whois 3.11 contains a stack-based buffer overflow vulnerability that allows remote attackers to execute arbitrary code by supplying oversized input to the IP address or domain field. Attackers can craft malicious input exceeding 658 bytes with shellcode to overwrite the structured exception handler and gain command execution when the application processes the input.	2026-06-01	9.8	CVE-2018-25427
Armcode--Arm Whois	Arm Whois 3.11 contains a buffer overflow vulnerability that allows local attackers to execute arbitrary code by overwriting the structured exception handler. Attackers can craft a malicious input file with a 672-byte offset to overwrite the nSEH and SEH pointers, enabling code execution through exception handler hijacking.	2026-06-01	8.4	CVE-2018-25432
armmember--ARMember Premium Membership Plugin, Content Restriction, Member Levels, User Profile & User signup	The ARMember Premium plugin for WordPress is vulnerable to an insecure password reset mechanism in all versions up to, and including, 7.3.1. The plugin stores a plaintext copy of the password reset key in the `arm_reset_password_key` user meta field when a user requests a password reset. This is in addition to the hashed key that WordPress core stores securely in `wp_users.user_activation_key`. The plaintext key stored in `wp_usermeta` can be used with the plugin's custom `armrp` reset action to set a new password for any user. Combined with another vulnerability such as SQL Injection (CVE-2026-5073, CVE-2026-5074), this makes it possible for unauthenticated attackers to extract the plaintext reset key and take over any user account, including administrators.	2026-06-02	9.8	CVE-2026-5076
armmember--ARMember Premium Membership Plugin, Content Restriction, Member Levels,	The ARMember Premium plugin for WordPress is vulnerable to SQL Injection via the 'order' parameter of the 'arm_directory_paging_action' AJAX action in all versions up to, and including, 7.3.1. This is due to insufficient escaping on the user-supplied 'order' and 'orderby' parameters and the lack of sufficient preparation on the existing SQL query in the `arm_get_directory_members()` function. This makes it possible for unauthenticated attackers to append additional SQL queries into already	2026-06-02	7.5	CVE-2026-5073

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
User Profile & User signup	existing queries that can be used to extract sensitive information from the database.			
AsyncHttpClient-async-http-client	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. Versions on the 2.x branch prior to 2.15.0 and the 3.x branch prior to 3.0.10 leak `Cookie` headers to cross-origin redirect targets. When following a redirect to a different origin, the `propagatedHeaders()` method in `Redirect30xInterceptor.java` strips `Authorization` and `Proxy-Authorization` headers but does not strip the `Cookie` header, causing session cookies and other sensitive cookie values to be sent to attacker-controlled servers. Versions 2.15.0 and 3.0.10 patch the issue.	2026-06-05	7.4	CVE-2026-45300
AWS--AWS Advanced Go Wrapper	An untrusted search path issue in the GlobalDatabasePlugin in the AWS Advanced Go Wrapper for Amazon Aurora PostgreSQL will allow a remote authenticated low-privilege actor to escalate privileges to those of another Amazon RDS user, including rds_superuser, via a crafted function created by the actor that runs when that user connects to the cluster through the affected wrapper. To remediate this issue, users should upgrade to the AWS Advanced Go Wrapper release 2026-05-26	2026-06-05	8	CVE-2026-11401
AWS--AWS Advanced JDBC Wrapper	An untrusted search path issue in the GlobalDatabasePlugin in the AWS Advanced JDBC Wrapper for Amazon Aurora PostgreSQL will allow a remote authenticated low-privilege actor to escalate privileges to those of another Amazon RDS user, including rds_superuser, via a crafted function created by the actor that runs when that user connects to the cluster through an affected wrapper. To remediate this issue, users should upgrade to AWS Advanced JDBC Wrapper version 4.0.1.	2026-06-05	8	CVE-2026-11400
AWS--Kiro IDE	Insufficient access control restrictions in the file write tool in Amazon Kiro IDE before version 0.11 might allow remote unauthenticated actors to execute arbitrary commands via crafted instructions that cause writes to execution-sensitive paths (such as .vscode/tasks.json), enabling auto-execution on folder open. To remediate this issue, users should upgrade to Kiro IDE version 0.11 or later.	2026-06-02	8.8	CVE-2026-10591
Axiomthemes--Confidant	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Axiomthemes Confidant allows PHP Local File Inclusion. This issue affects Confidant: from n/a through 1.4.	2026-06-02	8.1	CVE-2025-53440
Axiomthemes--Crafti	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Axiomthemes Crafti allows PHP Local File Inclusion. This issue affects Crafti: from n/a through 1.12.	2026-06-02	8.1	CVE-2025-58705
Axiomthemes--Fermentio	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Axiomthemes Fermentio allows PHP Local File Inclusion. This issue affects Fermentio: from n/a through 1.5.0.	2026-06-02	8.1	CVE-2025-58897
Axiomthemes--Racquet	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Axiomthemes Racquet allows PHP Local File Inclusion. This issue affects Racquet: from n/a through 1.12.0.	2026-06-02	8.1	CVE-2025-69369
Axiomthemes--Spin	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Axiomthemes Spin allows PHP Local File Inclusion. This issue affects Spin: from n/a through 1.8.	2026-06-02	8.1	CVE-2025-58707
Ben Balter--WP Document Revisions	Missing Authorization vulnerability in Ben Balter WP Document Revisions allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Document Revisions: from n/a before 4.0.0.	2026-06-01	7.5	CVE-2026-42677
Boost--Serialization	A flaw has been found in Boost Serialization up to 1.91. The impacted element is an unknown function. This manipulation causes improper validation of specified type of input. It is possible to initiate the attack remotely. The exploit has been published and may be used. The maintainer was notified on Aug 2025 and a disclosure deadline was set for	2026-06-07	7.3	CVE-2026-11460

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	90 days. The maintainer acknowledged but postponed indefinitely citing time concerns. No patch is currently available and the disclosure deadline has expired.			
browserstack--browserstack-runner	BrowserStack Runner through 0.9.5 contains a remote code execution vulnerability in the /_log HTTP handler that allows unauthenticated network-adjacent attackers to execute arbitrary code by submitting crafted JSON request bodies to the handler, which passes user-supplied data to vm.runInNewContext() combined with eval(). Attackers can escape the Node.js vm sandbox by leveraging a host-context Function reference through util.format to access the host process via this.constructor.constructor, achieving full remote code execution on the underlying system without any authentication.	2026-06-02	8.8	CVE-2026-49143
care2x--Care2x	Care2x 2.7 contains multiple SQL injection vulnerabilities that allow unauthenticated attackers to execute arbitrary SQL commands by manipulating the ck_config cookie parameter. Attackers can inject malicious SQL through the ck_config cookie in multiple endpoints including login.php, indexframe.php, and various module files to extract sensitive database information without authentication.	2026-06-04	8.2	CVE-2019-25728
Chanjet--CRM	A vulnerability was identified in Chanjet CRM 1.0. This affects an unknown part of the file /tools/jxf_dump_systable.php of the component HTTP GET Request Handler. Such manipulation of the argument gblOrgID leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-07	7.3	CVE-2026-11456
chartbrew--chartbrew	Chartbrew is an open-source web application that can connect directly to databases and APIs and use the data to create charts. In versions 4.9.0 through 5.0.0, an authenticated user with project-editor permissions can store arbitrary HTML/JavaScript in the `ChartDatasetConfig.legend` field. The payload is persisted verbatim in the database, propagated through the Chart.js rendering pipeline, and injected into the tooltip DOM element via an unguarded `innerHTML` assignment in `ChartTooltip.js`. Every unauthenticated viewer of the public dashboard triggers JavaScript execution on page load - no hover interaction is required. Browser-based Playwright verification confirmed `alert('localhost')` fires immediately and ` <td>2026-06-04</td> <td>7.6</td> <td>CVE-2026-41518</td>	2026-06-04	7.6	CVE-2026-41518
Chengdu Everbrite Network Technology--BeikeShop	A vulnerability was found in Chengdu Everbrite Network Technology BeikeShop up to 1.6.0.22. This impacts the function callback of the file plugins/Stripe/Controllers/StripeController.php of the component Stripe Plugin. Performing a manipulation of the argument Request results in improper authorization. The attack can be initiated remotely. The exploit has been made public and could be used. The patch is named 6719e0fc690ea0a998452092862e0f0a17c65968. It is suggested to install a patch to address this issue.	2026-06-07	7.3	CVE-2026-11462
Cisco--Cisco Catalyst SD-WAN Manager	A vulnerability in the CLI of Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an authenticated, local attacker to execute arbitrary commands as root by supplying a crafted file to the affected system. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by uploading a crafted file to the affected system. A successful exploit could allow the attacker to perform command injection attacks on an affected system and elevate their privileges as the root user. To exploit this vulnerability, the attacker must have netadmin privileges on the affected system. This would require valid credentials or exploitation of or . Cisco is not aware of successful exploitation by other methods. Cisco has observed limited cases where the exploitation of this bug resulted in a configuration change pushed to edge devices. Cisco recommends that customers upgrade to the fixed software that is documented in the that was published on May 14, 2026, and verify the configuration of the edge devices.	2026-06-04	7.8	CVE-2026-20245

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cisco--Cisco Unified Communications Manager	A vulnerability in Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to conduct server-side request forgery (SSRF) attacks through an affected device. This vulnerability is due to improper input validation for specific HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to write files to the underlying operating system that could be used later to elevate to root. Note: Cisco has assigned this security advisory a Security Impact Rating (SIR) of Critical rather than High as the score indicates. The reason is that exploitation of this vulnerability could result in an attacker elevating privileges to root. Note: To exploit this vulnerability, the WebDialer service must be enabled. WebDialer is disabled by default.	2026-06-03	8.6	CVE-2026-20230
Clash Verge Rev--clash-verge-service-ipc	clash-verge-service-ipc before 2.3.0 has a world-reachable IPC endpoint, leading to local privilege escalation.	2026-06-06	8.4	CVE-2026-26422
D-Link--DI-7001 MINI	A vulnerability was detected in D-Link DI-7001 MINI up to 19.09.19A1. Impacted is the function sprintf of the file /httpd_debug.asp of the component API. The manipulation of the argument Time results in stack-based buffer overflow. The attack may be performed from remote. The exploit is now public and may be used.	2026-06-01	8.8	CVE-2026-10270
Enderfga--claw-orchestrator	A weakness has been identified in Enderfga claw-orchestrator up to 3.5.5. This affects the function EmbeddedServer of the file src/embedded-server.ts of the component API Endpoint. This manipulation causes missing authentication. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 3.5.6 mitigates this issue. Patch name: d0b02a800aa0689d9428cc4cc170e0b6589fb2c3. The affected component should be upgraded.	2026-06-01	7.3	CVE-2026-10281
erzhongxmu--JeeWMS	A security flaw has been discovered in erzhongxmu JeeWMS up to 141740afb2ba14d441c82a833d0a418d07ca2d69. This vulnerability affects unknown code of the file /base-boot/jmreport/testConnection of the component JimuReport test-connection Endpoint. Performing a manipulation of the argument dbType/dbDriver/dbUrl/dbUsername/dbPassword results in injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-07	7.3	CVE-2026-11457
EventPrime--EventPrime	Missing Authorization vulnerability in EventPrime allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects EventPrime: from n/a through 4.3.2.0.	2026-06-02	7.5	CVE-2026-42669
Fox-themes--Prague	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fox-themes Prague allows Reflected XSS. This issue affects Prague: from n/a through 2.2.8.	2026-06-03	7.1	CVE-2025-15654
framework-y--Hybrid Composer	WordPress Hybrid Composer 1.4.6 contains an unauthenticated settings change vulnerability that allows unauthenticated attackers to modify WordPress options by exploiting the hc_ajax_save_option action. Attackers can send POST requests to the admin-ajax.php endpoint with the action parameter set to hc_ajax_save_option to enable user registration and set the default role to administrator, enabling account takeover.	2026-06-04	9.8	CVE-2019-25738
freedesktop--libinput	In libinput before 1.30.4 and 1.31.x before 1.31.3, libinput-device-group unescaped phys output can inject udev properties leading to arbitrary root code execution	2026-06-04	7.4	CVE-2026-50292
FreeIPMI--FreeIPMI	ipmi-oem in FreeIPMI before 1.6.18 has exploitable buffer overflows on response messages. The Intelligent Platform Management Interface (IPMI) specification defines a set of interfaces for platform management. It is	2026-06-03	7.5	CVE-2026-50031

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	implemented by a large number of hardware manufacturers to support system management. It is most commonly used for sensor reading (e.g., CPU temperatures through the ipmi-sensors command within FreeIPMI) and remote power control (the ipmipower command). The ipmi-oem client command implements a set of a IPMI OEM commands for specific hardware vendors. If a user has supported hardware, they may wish to use the ipmi-oem command to send a request to a server to retrieve specific information. Two subcommands "ipmi-oem dell get-active-directory-config" and "ipmi-oem fujitsu get-sel-entry-long-text" were found to have exploitable buffer overflows on response messages.			
froxlor--froxlor	Froxlor is open source server administration software. Version 2.3.6 contains a symlink-following flaw in the root-owned SSH key synchronization path used for customer FTP users. The provisioning code appends public keys to `~/ssh/authorized_keys` under a customer-controlled home directory without verifying that the target path is not a symbolic link. If an attacker controls a shell-enabled customer account and can modify files inside the assigned home directory, the attacker can replace `~/ssh/authorized_keys` with a symlink to `/root/.ssh/authorized_keys`. When Froxlor's privileged cron task later synchronizes SSH keys, it appends the attacker-supplied key into root's authorized key file, resulting in root SSH access. Version 2.3.7 contains a patch.	2026-06-04	8.8	CVE-2026-41236
froxlor--froxlor	Froxlor is open source server administration software. Prior to version 2.3.7, the `DomainZones.add` API endpoint does not sanitize newline characters in TXT record content. An authenticated customer with DNS editing enabled can inject newlines into TXT record values, which break out of the record line in the generated BIND zone file. This enables injection of arbitrary BIND directives (`\$INCLUDE`, `\$GENERATE`) and arbitrary DNS records (A, MX, CNAME) into the zone file written to disk by the DNS rebuild cron. This is an incomplete fix for CVE-2026-30932 (GHSA-x6w6-2xwp-3jh6), which patched the same newline injection for LOC, RP, SSHFP, and TLSA record types but did not patch TXT records. Version 2.3.7 contains an updated patch.	2026-06-04	7.6	CVE-2026-41234
Genetec Inc.-- Genetec Security Center	A high security vulnerability affecting Security Center main server installations has been identified. It could allow an attacker with local OS privileges to the main server to access the Server Admin credentials. A third party hired by Genetec found the issue. There is currently no evidence of active exploitation. This vulnerability is associated with specific installation package builds rather than the product version identifier alone. Certain versions (including 5.10.4.0, 5.11.3.0, 5.12.2.0 and 5.13.3.0) were released with both vulnerable and remediated installation packages under the same version number. Consequently, version-based comparison alone is insufficient to determine exposure. Only installations performed using vulnerable builds are affected. Remediated builds can be distinguished using verified installation package hashes. For the complete list of fixed build hashes, refer to the security advisory section.	2026-06-02	7.8	CVE-2026-40619
GL.iNet--GL-MT3000	A vulnerability was detected in GL.iNet GL-MT3000 4.4.5. This affects the function dlopen in the library /usr/lib/oui-httpd/rpc/ of the component Path Normalization Handler. Performing a manipulation of the argument dev_name results in command injection. It is possible to initiate the attack remotely. Upgrading to version 4.7 mitigates this issue. It is advisable to upgrade the affected component. The vendor confirms: " From version 4.7 onward, we have enabled method-level validation at the HTTP /rpc layer. nas-web.eject_disk is no longer in the whitelist of allowed methods. Consequently, directly calling eject_disk through the default /rpc endpoint returns Invalid params, preventing entry into subsequent dangerous functions and blocking the remote exploit chain described in the report."	2026-06-07	7.3	CVE-2026-11450

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
GL.iNet--GL-MT3000	A flaw has been found in GL.iNet GL-MT3000 4.4.5. This impacts the function sprintf of the file /cgi-bin/glc of the component FTP Protocol Handler. Executing a manipulation of the argument media_dir can lead to command injection. It is possible to launch the attack remotely. Upgrading to version 4.8.1 will fix this issue. You should upgrade the affected component. The vendor explains: "In version 4.8.1, before writing media_dir to the FTP configuration command, the code escapes single quotes using escape_single_quote(). The payloads in the report-which rely on closing a single quote, appending commands with a semicolon, and commenting out the tail with #-cannot escape execution under the current code path. We also verified this on a GLâ€™MT3000 device running firmware version 4.8.1 using similar payloads calling the /NAS_API_SET_PROTO_CONFIG interface. Although the interface returned success, the marker file intended to prove command execution was not created; the payload was written into /etc/vsftpd.conf only as ordinary configuration content and did not trigger any shell command execution. Therefore, with the current firmware version and default runtime environment, we could not reproduce the claimed "unauthorized command injection in set_proto_config"."	2026-06-07	7.3	CVE-2026-11451
GL.iNet--GL-MT3000	A vulnerability has been found in GL.iNet GL-MT3000 up to 4.4.5. Affected is the function FUN_0042e200 of the file /cgi-bin/glc of the component SET_USER_PWD Handler. The manipulation of the argument Password leads to command injection. The attack can be initiated remotely. Upgrading to version 4.8.1 is able to address this issue. The affected component should be upgraded. The vendor explains: " The current code escapes single quotes in the password parameter and handles it inside a shell singleâ€™quote context. The payloads in the report, which rely on \$() or backticks to trigger command substitution, are not executed under the current code path. We tested on a GLâ€™MT3000 device running firmware 4.8.1 using similar payloads, and no commandâ€™execution marker file was created."	2026-06-07	7.3	CVE-2026-11452
goauthentik--authentik	authentik is an open-source identity provider. Prior to versions 2025.12.5 and 2026.2.3, due to the implementation of stages in the SFE (Simple Flow Executor) in order to make the interface more compatible with legacy browsers, it was possible to use an XSS exploit in the AutosubmitStage. This issue has been patched in versions 2025.12.5 and 2026.2.3.	2026-06-02	9.3	CVE-2026-42849
goauthentik--authentik	authentik is an open-source identity provider. Prior to versions 2025.12.6, 2026.2.4, and 2026.5.1, the Source stage can be bypassed by sending an empty POST. This issue has been patched in versions 2025.12.6, 2026.2.4, and 2026.5.1.	2026-06-02	9.8	CVE-2026-49448
goauthentik--authentik	authentik is an open-source identity provider. Prior to versions 2025.12.5, 2026.2.3, and 2026.5.1, authentik's SAML Source ACS endpoint is vulnerable to XML Signature Wrapping when validating upstream SAML responses. An attacker with any account at the upstream IdP can reuse a valid signed assertion to authenticate as another federated user. This issue has been patched in versions 2025.12.5, 2026.2.3, and 2026.5.1.	2026-06-02	8.5	CVE-2026-47201
goauthentik--authentik	authentik is an open-source identity provider. Prior to versions 2025.12.6, 2026.2.4, and 2026.5.1, an attacker with the ability to change a source connection, and an account in one of the configured sources can log into any account. This issue has been patched in versions 2025.12.6, 2026.2.4, and 2026.5.1.	2026-06-02	8.8	CVE-2026-49443
goFrendiAsgard--No-CMS	No-Cms 1.0 contains an SQL injection vulnerability in the order_by parameter of the manage_privilege export endpoint that allows authenticated attackers to manipulate database queries. Attackers can submit POST requests to /nocms/main/manage_privilege/index/export with malicious SQL code in the order_by[0] parameter to extract sensitive database information.	2026-06-01	7.1	CVE-2018-25431

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Graphite project--Graphite	Graphite before 1.3.15 has an integer underflow and resultant out-of-bounds write via Graphite actions, because slotat does not ensure that an offset is within the allowed slot-map range.	2026-06-05	7.3	CVE-2026-50593
guardrails-ai--guardrails	Guardrails AI is a Python framework that helps build AI applications. On May 11, 2026 at approximately 6:00 PM Pacific, an attacker published a malicious version of `guardrails-ai` (0.10.1) to PyPI. Aany user who installed `guardrails-ai==0.10.1` from PyPI on May 11, 2026 may be affected. Security researchers identified the malicious package within approximately 2 hours of publication, and PyPI quarantined the repository. Based on our telemetry, Guardrails AI maintainers have observed no requests to Guardrails AI infrastructure originating from the malicious 0.10.1 version, and a review of system and access logs has produced no evidence of user data exfiltration through their systems. Users should upgrade to version 0.10.2 or downgrade to version 0.10.0, both of which are unaffected. Those who installed version 0.10.1 should rotate any credentials accessible from their machine (GitHub PATs, cloud provider keys, package registry tokens, API keys) and audit their GitHub account for unauthorized workflows or repositories.	2026-06-05	9.6	CVE-2026-45758
H3C--Magic B0	A security vulnerability has been detected in H3C Magic B0 up to 100R002. The affected element is the function SetMobileAPIInfoByld of the file /goform/aspForm. Such manipulation of the argument param leads to stack-based buffer overflow. The attack may be performed from remote. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-01	8.8	CVE-2026-10259
haxtheweb--haxcms-php	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Prior to version 26.0.0 of HAX CMS PHP, the `saveFile` endpoint validates upload extensions case-insensitively and writes the filename to disk verbatim, but the `.htaccess` rule that forces `Content-Disposition: attachment` on HTML files is case-sensitive. An HTML file uploaded with an uppercase extension (`.HTML`, `.Html`, `.HTM`) is still served as `text/html` but the forced-download header never applies, so the browser renders it inline and executes any embedded JavaScript in the HAXcms origin. This bypasses the mitigation shipped for CVE-2026-22704. Version 26.0.0 contains a fix.	2026-06-05	8.7	CVE-2026-46392
haxtheweb--haxcms-php	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Versions prior to 26.0.1 use `uniqid` for generating salts, which is unsuitable. Version 26.0.1 fixes the issue.	2026-06-05	7.5	CVE-2026-46493
HCL--Hive	HCL Hive Telco Observability is affected by a Required directives missing from the CSP issue is detected in keycloak component of the web application. Missing essential directives can leave a site vulnerable.	2026-06-04	8.1	CVE-2025-59874
HCL--iControl	HCL iControl was affected by Export CSV - CSV Injection vulnerability. It is vulnerable to a reflected cross-site scripting vulnerability. This was caused by an insufficient sanitation of input parameters. .	2026-06-04	7.1	CVE-2025-52612
hippooo--Hippoo Mobile App for WooCommerce	The Hippoo Mobile App for WooCommerce plugin for WordPress is vulnerable to Authentication Bypass leading to Administrator Account Takeover in all versions up to and including 1.9.4. This is due to a logic conflation in HippooPermissions::get_user_permissions(), which returns the same null sentinel for both administrators and unauthenticated visitors - a value that HippooPermissions::has_role_access() unconditionally interprets as full administrator access - causing override_extension_permission_callback() to assign __return_true as the permission callback for every WordPress and WooCommerce REST route cloned under /wc-hippoo/v1/ext/ by HippooControllerWithAuth::re_register_external_routes(), while the block_unauthorized_access() pre-dispatch guard fails to block unauthenticated users for the same reason. This makes it possible for unauthenticated attackers to invoke any core REST endpoint without credentials - most critically, sending a POST request to /wc-hippoo/v1/ext/wp/v2/users/<id> with a {"password":"<new_password>"}	2026-06-05	9.8	CVE-2026-10580

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	body to reset the password of any WordPress user, including the site administrator, and gain full administrative control of the site.			
horizon921--mcpilot	A security flaw has been discovered in horizon921 mcpilot 0.1.0. The impacted element is an unknown function of the file client/src/app/api/mcp/call/route.ts of the component MCP API Call Endpoint. The manipulation of the argument serverBaseUrl results in server-side request forgery. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	7.3	CVE-2026-10280
IBM--i Access Family	IBM i Access Family 1.1.5.0 through 1.1.9.12 IBM i Access Client Solutions (ACS) is vulnerable to remote code execution when configured to listen for requests from IBM i Navigator.	2026-06-01	8.8	CVE-2026-7770
IBM--WebSphere Application Server	IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to identity spoofing.	2026-06-01	9.1	CVE-2026-8644
IBM--WebSphere Application Server	IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to remote code execution caused by the bypass of security controls.	2026-06-01	9	CVE-2026-9311
IBM--WebSphere Application Server	IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to potential remote code execution due to deserialization of untrusted data via JAX-WS endpoints with WS-Security.	2026-06-01	9	CVE-2026-9319
IBM--WebSphere Application Server	IBM WebSphere Application Server 9.0, and 8.5 is affected by an improper validation of user-supplied data during deserialization using the SAML Web Single Sign-On component. This could result in remote code execution via a crafted HTTP request when combined with a suitable gadget chain.	2026-06-01	8.5	CVE-2026-9330
itsourcecode--Online Blood Bank Management System	A vulnerability was identified in itsourcecode Online Blood Bank Management System 1.0. Impacted is an unknown function of the file /admin/viewrequest.php. Such manipulation of the argument ID leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	2026-06-01	7.3	CVE-2026-10249
itsourcecode--Online Blood Bank Management System	A security flaw has been discovered in itsourcecode Online Blood Bank Management System 1.0. The affected element is an unknown function of the file /admin/campsdetails.php. Performing a manipulation of the argument hospital results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks.	2026-06-01	7.3	CVE-2026-10250
itsourcecode--Online House Rental System	A weakness has been identified in itsourcecode Online House Rental System 1.0. The impacted element is an unknown function of the file /ajax.php?action=login. Executing a manipulation of the argument Username can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	2026-06-01	7.3	CVE-2026-10251
itsourcecode--Online House Rental System	A security vulnerability has been detected in itsourcecode Online House Rental System 1.0. This affects an unknown function of the file /manage_tenant.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	2026-06-01	7.3	CVE-2026-10252
itsourcecode--Online House Rental System	A vulnerability was detected in itsourcecode Online House Rental System 1.0. This impacts an unknown function of the file /manage_payment.php. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	2026-06-01	7.3	CVE-2026-10253
Ivanti--Neurons for ITSM (On-Premises)	An Improper Access Control vulnerability in Ivanti Neurons for ITSM (cloud and on-premises) allows a remote authenticated attacker to gain administrative access.	2026-06-01	8.8	CVE-2026-9614
igwhite33--Google Review Slider	WordPress Plugin Google Review Slider 6.1 contains a time-based blind SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the 'tid'	2026-06-04	8.2	CVE-2019-25745

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	parameter. Attackers can send GET requests to the admin interface with malicious 'tid' values to extract sensitive database information using time-based blind SQL injection techniques.			
ghorowitz--Content Visibility for Divi Builder	The Content Visibility for Divi Builder plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 4.02 via the 'et_pb_text' shortcode 'cvdb_content_visibility_check' parameter. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute code on the server.	2026-06-02	8.8	CVE-2026-1829
JingDong--JD Cloud Box AX6600	A security vulnerability has been detected in JingDong JD Cloud Box AX6600 4.5.3.r4546. The impacted element is the function set_macfilter of the file /sbin/jdcweb_rpc. The manipulation leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-06	8.8	CVE-2026-11413
Jinher--OA	A security vulnerability has been detected in Jinher OA 1.0. This affects an unknown function of the file nextselectplan.aspx. Such manipulation of the argument httpOID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-06	7.3	CVE-2026-11435
Joomlaextension s--JE Photo Gallery	Joomla Component JE Photo Gallery 1.1 contains an SQL injection vulnerability that allows unauthenticated attackers to extract database information by injecting malicious SQL code through the categoryid parameter. Attackers can send GET requests to index.php with crafted categoryid values in the com_jephotogallery component to execute arbitrary SQL queries and retrieve sensitive data like usernames and password hashes.	2026-06-01	8.2	CVE-2018-25433
jxxghp--MoviePilot	MoviePilot contains a path traversal vulnerability in the AliPan, U115, and Rclone cloud storage download handlers where the local destination path is constructed by concatenating the configured download directory with a filename taken directly from remote cloud API metadata without basename normalization or path validation. An attacker who controls a filename returned by a remote cloud storage API can include traversal sequences ../ in the filename to cause downloaded content to be written outside the configured download directory, potentially overwriting arbitrary files including configuration or plugin files reachable by the application process.	2026-06-05	8.1	CVE-2026-11416
kiteworks--Secure Data Forms	Kiteworks is a private data network (PDN). Prior to version 9.3.0, a reflected XSS vulnerability in Kiteworks Secure Data Forms could allow an external attacker to trick a user into executing arbitrary JavaScript code. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	2026-06-01	8.2	CVE-2026-24751
kiteworks--Secure Data Forms	Kiteworks is a private data network (PDN). Prior to version 9.3.0, a reflected XSS vulnerability in Kiteworks Secure Data Forms could allow an external attacker to trick a user into executing arbitrary JavaScript code. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	2026-06-01	8.2	CVE-2026-24752
kiteworks--Secure Data Forms	Kiteworks is a private data network (PDN). Prior to version 9.3.0, multiple SQL Injection vulnerabilities in Kiteworks Secure Data Forms could be exploited by an authenticated attacker with the FormBuilder role to retrieve information on or modify other users' form definitions and some global configuration parameters. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	2026-06-01	7.6	CVE-2026-24782
Kurt Software Studio--WriteUp Mobile App	Improper Access Control, Missing Authorization vulnerability in Kurt Software Studio WriteUp Mobile App allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects WriteUp Mobile App: from 1.3.0 through 04062026.	2026-06-04	8.8	CVE-2026-5228
Labf--LabF nfsAxe	LabF nfsAxe 3.7 Ping Client contains a buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying a malicious payload in the Host IP field. Attackers can craft a specially formatted input	2026-06-04	8.4	CVE-2019-25736

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	file with shellcode and overwrite the return address to execute calc.exe or other arbitrary commands.			
langroid--langroid	Langroid is a framework for building large-language-model-powered applications. Prior to version 0.63.0, SQLChatAgent executes SQL produced by an LLM, which is influenceable by prompt injection. When configured with a database role that has privileges enabling code execution or filesystem access (e.g., PostgreSQL pg_execute_server_program, MySQL FILE, MSSQL xp_cmdshell), an attacker who can shape the agent's input - including indirectly via data returned to the LLM - can coerce execution of dialect-specific primitives such as `COPY ... FROM PROGRAM`, achieving RCE on the database host. Fixed in v0.63.0 by defaulting SQLChatAgent to a SELECT-only sqlglot-parsed statement allowlist with a dialect-aware dangerous-pattern blacklist; allow_dangerous_operations=True restores the previous unrestricted behavior for trusted deployments.	2026-06-01	9.8	CVE-2026-25879
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_inner: Fix IPv6 inner_thoff desync In nft_inner_parse_l2l3(), when processing inner IPv6 packets, ipv6_find_hdr() correctly computes the transport header offset traversing all extension headers, but the result is immediately overwritten with nhoff + sizeof(_ip6h) (40 bytes), which only accounts for the IPv6 base header. This creates a desync between inner_thoff (wrong - points to extension header start) and l4proto (correct - e.g., IPPROTO_TCP), enabling transport header forgery and potential firewall bypass. This issue affects stable versions from Linux 6.2. For comparison, the normal (non-inner) IPv6 path correctly preserves ipv6_find_hdr()'s result. Removing the incorrect overwrite ensures that ipv6_find_hdr()'s calculated transport header offset is preserved, thereby fixing the desynchronization.	2026-06-03	9.1	CVE-2026-46244
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: inet: RAW sockets using IPPROTO_RAW MUST drop incoming ICMP Yizhou Zhao reported that simply having one RAW socket on protocol IPPROTO_RAW (255) was dangerous. socket(AF_INET, SOCK_RAW, 255); A malicious incoming ICMP packet can set the protocol field to 255 and match this socket, leading to FNHE cache changes. inner = IP(src="192.168.2.1", dst="8.8.8.8", proto=255)/Raw("TEST") pkt = IP(src="192.168.1.1", dst="192.168.2.1")/ICMP(type=3, code=4, nexthopmtu=576)/inner "man 7 raw" states: A protocol of IPPROTO_RAW implies enabled IP_HDRINCL and is able to send any IP protocol that is specified in the passed header. Receiving of all IP protocols via IPPROTO_RAW is not possible using raw sockets. Make sure we drop these malicious packets.	2026-06-03	9.1	CVE-2026-46266
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix block_group_tree dirty_list corruption When the incompat flag EXTENT_TREE_V2 is set, we unconditionally add the block group tree to the switch_commits list before calling switch_commit_roots, as we do for the tree root and the chunk root. However, the block group tree uses normal root dirty tracking and in any transaction that does an allocation and dirties a block group, the block group root will already be linked to a list by the dirty_list field and this use of list_add_tail() is invalid and corrupts the prev/next members of block_group_root->dirty_list. This is apparent on a subsequent list_del on the prev if we enable CONFIG_DEBUG_LIST: [32.1571] -----[cut here]----- [32.1572] list_del corruption. next->prev should beffff958890202538, but was ffff9588992bd538. (next=ffff958890201538) [32.1575] WARNING: lib/list_debug.c:65 at 0x0, CPU#3: sync/607 [32.1583] CPU: 3 UID: 0 PID: 607 Comm: sync Not tainted 6.18.0 #24PREEMPT(none) [32.1585] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS1.17.0-4.fc41 04/01/2014 [32.1587] RIP: 0010: __list_del_entry_valid_or_report+0x108/0x120 [32.1593] RSP: 0018: fffffaa288287fdd0 EFLAGS: 00010202 [32.1594] RAX: 0000000000000001 RBX: ffff95889326e800 RCX: ffff958890201538	2026-06-03	8.4	CVE-2026-46251

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	[32.1596] RDX: ffff9588992bd538 RSI: ffff958890202538 RDI: ffffffff82a41e00 [32.1597] RBP: ffff958890202538 R08: ffffffff828fc1e8 R09: 00000000ffffefff [32.1599] R10: ffffffff8288c200 R11: ffffffff828e4200 R12: ffff958890201538 [32.1601] R13: ffff95889326e958 R14: ffff958895c24000 R15: ffff958890202538 [32.1603] FS: 00007f0c28eb5740(0000) GS: ffff958af2bd2000(0000) knlGS: 0000000000000000 [32.1605] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [32.1607] CR2: 00007f0c28e8a3cc CR3: 0000000109942005 CR4: 0000000000370ef0 [32.1609] Call Trace: [32.1610] <TASK> [32.1611] switch_commit_roots+0x82/0x1d0 [btrfs] [32.1615] btrfs_commit_transaction+0x968/0x1550 [btrfs] [32.1618] ? btrfs_attach_transaction_barrier+0x23/0x60 [btrfs] [32.1621] __iterate_supers+0xe8/0x190 [32.1622] ? __pfx_sync_fs_one_sb+0x10/0x10 [32.1623] ksys_sync+0x63/0xb0 [32.1624] __do_sys_sync+0xe/0x20 [32.1625] do_syscall_64+0x73/0x450 [32.1626] entry_SYSCALL_64_after_hwframe+0x76/0x7e [32.1627] RIP: 0033:0x7f0c28d05d2b [32.1632] RSP: 002b:00007ffc9d988048 EFLAGS: 00000246 ORIG_RAX: 00000000000000a2 [32.1634] RAX: ffffffff8da RBX: 00007ffc9d988228 RCX: 00007f0c28d05d2b [32.1636] RDX: 00007f0c28e02301 RSI: 00007ffc9d989b21 RDI: 00007f0c28dba90d [32.1637] RBP: 0000000000000001 R08: 0000000000000001 R09: 0000000000000000 [32.1639] R10: 0000000000000000 R11: 0000000000000246 R12: 000055b96572cb80 [32.1641] R13: 000055b96572b19f R14: 00007f0c28dfa434 R15: 000055b96572b034 [32.1643] </TASK> [32.1644] irq event stamp: 0 [32.1644] hardirqs last enabled at (0): [0000000000000000] 0x0 [32.1646] hardirqs last disabled at (0): [ffffffffff81298817] copy_process+0xb37/0x2260 [32.1648] softirqs last enabled at (0): [ffffffffff81298817] copy_process+0xb37/0x2260 [32.1650] softirqs last disabled at (0): [0000000000000000] 0x0 [32.1652] ---[end trace 0000000000000000]--- Furthermore, this list corruption eventually (when we happen to add a new block group) results in getting the switch_commits and dirty_cowonly_roots lists mixed up and attempting to call update_root on the tree root which can't be found in the tree root, resulting in a transaction abort: [87.8269] BTRFS critical (device nvme1n1): unable to find root key (1 0 0) in tree 1 [87.8272] -----[cut here]----- [87.8274] BTRFS: Transaction aborted (error -117) [87.8275] WARNING: fs/btrfs/root-tree.c:153 at 0x0, CPU#4: sync/703 [87.8285] CPU: 4 UID: 0 PID: 703 Comm: sync Not tainted 6.18.0 #25 PREEMPT(none) [87.8287] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.17.0-4.fc41 0 ---truncated---			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xen/pf: Fix sysfs initialization In case of devm_add_action_or_reset() failure the provided cleanup action will be run immediately on the not yet initialized kobject. This may lead to errors like: [] kobject: '(null)' (ffff10001393608e0): is not initialized, yet kobject_put() is being called. [] WARNING: lib/kobject.c:734 at kobject_put+0xd9/0x250, CPU#0: kworker/0:0/9 [] RIP: 0010:kobject_put+0xdf/0x250 [] Call Trace: [] xe_sriov_pf_sysfs_init+0x21/0x100 [xe] [] xe_sriov_pf_init_late+0x87/0x2b0 [xe] [] xe_sriov_init_late+0x5f/0x2c0 [xe] [] xe_device_probe+0x5f2/0xc20 [xe] [] xe_pci_probe+0x396/0x610 [xe] [] local_pci_probe+0x47/0xb0 [] refcount_t: underflow; use-after-free. [] WARNING: lib/refcount.c:28 at refcount_warn_saturate+0x68/0xb0, CPU#0: kworker/0:0/9 [] RIP: 0010:refcount_warn_saturate+0x68/0xb0 [] Call Trace: [] kobject_put+0x174/0x250 [] xe_sriov_pf_sysfs_init+0x21/0x100 [xe] [] xe_sriov_pf_init_late+0x87/0x2b0 [xe] [] xe_sriov_init_late+0x5f/0x2c0 [xe] [] xe_device_probe+0x5f2/0xc20 [xe] [] xe_pci_probe+0x396/0x610	2026-06-03	8.8	CVE-2026-46264

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	[xe] [] local_pci_probe+0x47/0xb0 Fix that by calling kobject_init() and kobject_add() separately and register cleanup action after the kobject is initialized. Also make this cleanup registration a part of the create helper to fix another mistake, as in the loop we were wrongly passing parent kobject while registering cleanup action, and this resulted in some undetected leaks. (cherry picked from commit 98b16727f07e26a5d4de84d88805ce7ffcfd324)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: power: supply: rt9455: Fix use-after-free in power_supply_changed() Using the `devm_` variant for requesting IRQ_before_ the `devm_` variant for allocating/registering the `power_supply` handle, means that the `power_supply` handle will be deallocated/unregistered_before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where an interrupt can fire just_after_ the `power_supply` handle has been freed, *but* just_before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `power_supply_changed()` with a freed `power_supply` handle. Which usually crashes the system or otherwise silently corrupts the memory... Note that there is a similar situation which can also happen during `probe()`; the possibility of an interrupt firing_before_ registering the `power_supply` handle. This would then lead to the nasty situation of using the `power_supply` handle *uninitialized* in `power_supply_changed()`. Fix this racy use-after-free by making sure the IRQ is requested_after_ the registration of the `power_supply` handle.	2026-06-03	8.4	CVE-2026-46270
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ibmveth: Disable GSO for packets with small MSS Some physical adapters on Power systems do not support segmentation offload when the MSS is less than 224 bytes. Attempting to send such packets causes the adapter to freeze, stopping all traffic until manually reset. Implement ndo_features_check to disable GSO for packets with small MSS values. The network stack will perform software segmentation instead. The 224-byte minimum matches ibmvnic commit <f10b09ef687f> ("ibmvnic: Enforce stronger sanity checks on GSO packets") which uses the same physical adapters in SEA configurations. The issue occurs specifically when the hardware attempts to perform segmentation (gso_segs > 1) with a small MSS. Single-segment GSO packets (gso_segs == 1) do not trigger the problematic LSO code path and are transmitted normally without segmentation. Add an ndo_features_check callback to disable GSO when MSS < 224 bytes. Also call vlan_features_check() to ensure proper handling of VLAN packets, particularly QinQ (802.1ad) configurations where the hardware parser may not support certain offload features. Validated using iptables to force small MSS values. Without the fix, the adapter freezes. With the fix, packets are segmented in software and transmission succeeds. Comprehensive regression testing completedd (MSS tests, performance, stability).	2026-06-03	8.6	CVE-2026-46273
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: smb: client: reject userspace cifs.spnego descriptions cifs.spnego key descriptions contain authority-bearing fields such as pid, uid, creduid, and upcall_target that cifs.upcall treats as kernel-originating inputs. However, userspace can also create keys of this type through request_key(2) or add_key(2), allowing those fields to be supplied without CIFS origin. Only accept cifs.spnego descriptions while CIFS is using its private spnego_cred to request the key.	2026-06-01	7.1	CVE-2026-46243
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: MIPS: Work around LLVM bug when gp is used as global register variable On MIPS, __current_thread_info is defined as global register variable locating in \$gp, and is simply assigned with new address during kernel relocation. This however is broken with LLVM, which always restores \$gp if it finds \$gp is clobbered in any form, including when intentionally through a global	2026-06-03	7.3	CVE-2026-46250

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	register variable. This is against GCC's documentation[1], which requires a callee-saved register used as global register variable not to be restored if it's clobbered. As a result, \$gp will continue to point to the unrelocated kernel after the epilog of relocate_kernel(), leading to an early crash in init_idle, [0.000000] CPU 0 Unable to handle kernel paging request at virtual address 0000000000000000, epc == ffffffff81afada8, ra == ffffffff81afad90 [0.000000] Oops[#1]: [0.000000] CPU: 0 UID: 0 PID: 0 Comm: swapper Tainted: G W 6.19.0-rc5-00262-gd3eeb99bbc99-dirty #188 VOLUNTARY [0.000000] Tainted: [W]=WARN [0.000000] Hardware name: loongson,loongson64v-4core-virtio [0.000000] \$ 0 : 0000000000000000 0000000000000000 0000000000000001 0000000000000000 [0.000000] \$ 4 : ffffffff80b80ec0 ffffffff80b53d48 0000000000000000 000000000000f4240 [0.000000] \$ 8 : 00000000000000100 ffffffff81d82f80 ffffffff81d82f80 0000000000000001 [0.000000] \$12 : 0000000000000000 ffffffff81776f58 000000000000005da 0000000000000002 [0.000000] \$16 : ffffffff80b80e40 0000000000000000 ffffffff80b81614 9800000005dfbe80 [0.000000] \$20 : 00000000540000e0 ffffffff81980000 0000000000000000 ffffffff80f81c80 [0.000000] \$24 : 00000000000000a26 ffffffff8114fb90 [0.000000] \$28 : ffffffff80b50000 ffffffff80b53d40 0000000000000000 ffffffff81afad90 [0.000000] Hi : 0000000000000000 [0.000000] Lo : 0000000000000000 [0.000000] epc : ffffffff81afada8 init_idle+0x130/0x270 [0.000000] ra : ffffffff81afad90 init_idle+0x118/0x270 [0.000000] Status: 540000e2 KX SX UX KERNEL EXL [0.000000] Cause : 00000008 (ExcCode 02) [0.000000] BadVA : 0000000000000000 [0.000000] PrId : 00006305 (ICT Loongson-3) [0.000000] Process swapper (pid: 0, threadinfo=(____ptrval____), task=(____ptrval____), tls=0000000000000000) [0.000000] Stack : 9800000005dfbf00 ffffffff8178e950 0000000000000000 0000000000000000 [0.000000] 0000000000000000 ffffffff81970000 0000000000000003f ffffffff810a6528 [0.000000] 0000000000000001 9800000005dfbe80 9800000005dfbf00 ffffffff81980000 [0.000000] ffffffff810a6450 ffffffff81afb6c0 0000000000000000 ffffffff810a2258 [0.000000] ffffffff81d82ec8 ffffffff8198d010 ffffffff81b67e80 ffffffff8197dd98 [0.000000] ffffffff81d81c80 ffffffff81930000 0000000000000040 0000000000000000 [0.000000] 0000000000000000 0000000000000000 0000000000000000 [0.000000] 0000000000000000 0000000000000009e ffffffff9fc01000 0000000000000000 [0.000000] 0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000 [0.000000] 0000000000000000 0000000000000000 [0.000000] 0000000000000000 ffffffff81ae86dc ffffffff81b3c741 0000000000000002 [0.000000] ... [0.000000] Call Trace: [0.000000] [<fffffff81afada8>] init_idle+0x130/0x270 [0.000000] [<fffffff81afb6c0>] sched_init+0x5c8/0x6c0 [0.000000] [<fffffff81ae86dc>] start_kernel+0x27c/0x7a8 This bug has been reported to LLVM[2] and affects version from (at least) 18 to 21. Let's work around this by using inline assembly to assign \$gp before a fix is widely available.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: pstore/ram: fix buffer overflow in persistent_ram_save_old() persistent_ram_save_old() can be called multiple times for the same persistent_ram_zone (e.g., via ramoops_pstore_read -> ramoops_get_next_prz for PSTORE_TYPE_DMESG records). Currently, the function only allocates prz->old_log when it is NULL, but it unconditionally updates prz->old_log_size to the current buffer size and then performs memcpy_fromio() using this new size. If the buffer size has grown since the first allocation (which can happen across different kernel boot cycles), this leads to: 1. A heap buffer overflow (OOB write) in the memcpy_fromio() calls 2. A subsequent OOB read when ramoops_pstore_read() accesses the buffer using the incorrect (larger) old_log_size The KASAN splat would look similar to: BUG: KASAN: slab-out-of-bounds in ramoops_pstore_read+0x...	2026-06-03	7.8	CVE-2026-46253

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Read of size N at addr ... by task ... The conditions are likely extremely hard to hit: 0. Crash with a ramoops write of less-than-record-max-size bytes. 1. Reboot: ramoops registers, pstore_get_records(0) reads old crash, allocates old_log with size X 2. Crash handler registered, timer started (if pstore_update_ms >= 0) 3. Oops happens (non-fatal, system continues) 4. pstore_dump() writes oops via ramoops_pstore_write() size Y (>X) 5. pstore_new_entry = 1, pstore_timer_kick() called 6. System continues running (not a panic oops) 7. Timer fires after pstore_update_ms milliseconds 8. pstore_timefunc() â†’ schedule_work() â†’ pstore_dowork() â†’ pstore_get_records(1) 9. ramoops_get_next_prz() â†’ persistent_ram_save_old() 10. buffer_size() returns Y, but old_log is X bytes 11. Y > X: memcpy_fromio() overflows heap Requirements: - a prior crash record exists that did not fill the record size (almost impossible since the crash handler writes as much as it can possibly fit into the record, capped by max record size and the kmsg buffer almost always exceeds the max record size) - pstore_update_ms >= 0 (disabled by default) - Non-fatal oops (system survives) Free and reallocate the buffer when the new size differs from the previously allocated size. This ensures old_log always has sufficient space for the data being copied.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: procs: fix missing RCU protection when reading real_parent in do_task_stat() When reading /proc/[pid]/stat, do_task_stat() accesses task->real_parent without proper RCU protection, which leads to: cpu 0 cpu 1 ----- do_task_stat var = task->real_parent release_task call_rcu(delayed_put_task_struct) task_tgid_nr_ns(var) rcu_read_lock <--- Too late to protect task->real_parent! task_pid_ptr <--- UAF! rcu_read_unlock This patch uses task_ppid_nr_ns() instead of task_tgid_nr_ns() to add proper RCU protection for accessing task->real_parent.	2026-06-03	7.8	CVE-2026-46259
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: Fix out-of-bound access in fib6_add_rt2node(). syzbot reported out-of-bound read in fib6_add_rt2node(). [0] When IPv6 route is created with RTA_NH_ID, struct fib6_info does not have the trailing struct fib6_nh. The cited commit started to check liter->fib6_nh->fib_nh_gw_family to ensure that rt6_qualify_for_ecmp() will return false for iter. If iter->nh is not NULL, rt6_qualify_for_ecmp() returns false anyway. Let's check iter->nh before reading iter->fib6_nh and avoid OOB read. [0]: BUG: KASAN: slab-out-of-bounds in fib6_add_rt2node+0x349c/0x3500 net/ipv6/ip6_fib.c:1142 Read of size 1 at addr ffff8880384ba6de by task syz.0.18/5500 CPU: 0 UID: 0 PID: 5500 Comm: syz.0.18 Not tainted syzkaller #0 PREEMPT(full) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0xe8/0x150 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xba/0x230 mm/kasan/report.c:482 kasan_report+0x117/0x150 mm/kasan/report.c:595 fib6_add_rt2node+0x349c/0x3500 net/ipv6/ip6_fib.c:1142 fib6_add_rt2node_nh net/ipv6/ip6_fib.c:1363 [inline] fib6_add+0x910/0x18c0 net/ipv6/ip6_fib.c:1531 __ip6_ins_rt net/ipv6/route.c:1351 [inline] ip6_route_add+0xde/0x1b0 net/ipv6/route.c:3957 inet6_rtm_newroute+0x268/0x19e0 net/ipv6/route.c:5660 rtnetlink_rcv_msg+0x7d5/0xbe0 net/core/rtnetlink.c:6958 netlink_rcv_skb+0x232/0x4b0 net/netlink/af_netlink.c:2550 netlink_unicast_kernel net/netlink/af_netlink.c:1318 [inline] netlink_unicast+0x80f/0x9b0 net/netlink/af_netlink.c:1344 netlink_sendmsg+0x813/0xb40 net/netlink/af_netlink.c:1894 sock_sendmsg_nosec net/socket.c:727 [inline] __sock_sendmsg net/socket.c:742 [inline] ____sys_sendmsg+0xa68/0xad0 net/socket.c:2592	2026-06-03	7.8	CVE-2026-46260

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	__sys_sendmsg+0x2a5/0x360 net/socket.c:2646 __sys_sendmsg net/socket.c:2678 [inline] __do_sys_sendmsg net/socket.c:2683 [inline] __se_sys_sendmsg net/socket.c:2681 [inline] __x64_sys_sendmsg+0x1bd/0x2a0 net/socket.c:2681 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xe2/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f9316b9aeb9 Code: ff c3 66 2e 0f 1f 84 00 00 00 00 0f 1f 44 00 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 e8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffd8809b678 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffda RBX: 00007f9316e15fa0 RCX: 00007f9316b9aeb9 RDX: 0000000000000000 RSI: 0000200000004380 RDI: 0000000000000003 RBP: 00007f9316c08c1f R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007f9316e15fac R14: 00007f9316e15fa0 R15: 00007f9316e15fa0 </TASK> Allocated by task 5499: kasan_save_stack mm/kasan/common.c:57 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:78 poison_kmalloc_redzone mm/kasan/common.c:398 [inline] __kasan_kmalloc+0x93/0xb0 mm/kasan/common.c:415 kasan_kmalloc include/linux/kasan.h:263 [inline] __do_kmalloc_node mm/slub.c:5657 [inline] __kmalloc_noprof+0x40c/0x7e0 mm/slub.c:5669 kmalloc_noprof include/linux/slab.h:961 [inline] kzalloc_noprof include/linux/slab.h:1094 [inline] fib6_info_alloc+0x30/0xf0 net/ipv6/ip6_fib.c:155 ip6_route_info_create+0x142/0x860 net/ipv6/route.c:3820 ip6_route_add+0x49/0x1b0 net/ipv6/route.c:3949 inet6_rtm_newroute+0x268/0x19e0 net/ipv6/route.c:5660 rtnetlink_rcv_msg+0x7d5/0xbe0 net/core/rtnetlink.c:6958 netlink_rcv_skb+0x232/0x4b0 net/netlink/af_netlink.c:2550 netlink_unicast_kernel net/netlink/af_netlink.c:1318 [inline] netlink_unicast+0x80f/0x9b0 net/netlink/af_netlink.c:1344 netlink_sendmsg+0x813/0xb40 net/netlink/af_netlink.c:1894 sock_sendmsg_nosec net/socket.c:727 [inline] __sock_sendmsg net/socket.c:742 [inline] ____sys_sendmsg+0xa68/0xad0 net/socket.c:2592 ____sys_s ---truncated---			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix out-of-bounds stream encoder index v3 eng_id can be negative and that stream_enc_regs[] can be indexed out of bounds. eng_id is used directly as an index into stream_enc_regs[], which has only 5 entries. When eng_id is 5 (ENGINE_ID_DIGF) or negative, this can access memory past the end of the array. Add a bounds check using ARRAY_SIZE() before using eng_id as an index. The unsigned cast also rejects negative values. This avoids out-of-bounds access. Fixes the below smatch error: dcn*_resource.c: stream_encoder_create() may index stream_enc_regs[eng_id] out of bounds (size 5). drivers/gpu/drm/amd/amdgpu/./display/dc/resource/dcn351/dcn351_resource.c 1246 static struct stream_encoder *dcn35_stream_encoder_create(1247 enum engine_id eng_id, 1248 struct dc_context *ctx) 1249 { ... 1255 1256 /* Mapping of VPG, AFMT, DME register blocks to DIO block instance */ 1257 if (eng_id <= ENGINE_ID_DIGF) { ENGINE_ID_DIGF is 5. should <= be <? Unrelated but, ugh, why is Smatch saying that "eng_id" can be negative? end_id is type signed long, but there are checks in the caller which prevent it from being negative. 1258 vpg_inst = eng_id; 1259 afmt_inst = eng_id; 1260 } else 1261 return NULL; 1262 ... 1281 1282 dcn35_dio_stream_encoder_construct(enc1, ctx, ctx->dc_bios, 1283 eng_id, vpg, afmt, --> 1284 &stream_enc_regs[eng_id], ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ This stream_enc_regs[] array has 5 elements so we are one element beyond the end of the array. ... 1287 return &enc1-	2026-06-03	7.8	CVE-2026-46263

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	>base; 1288 } v2: use explicit bounds check as suggested by Roman/Dan; avoid unsigned int cast v3: The compiler already knows how to compare the two values, so the cast (int) is not needed. (Roman)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/hns: Fix WQ_MEM_RECLAIM warning When sunrpc is used, if a reset triggered, our wq may lead the following trace: workqueue: WQ_MEM_RECLAIM xprtiod:xprt_rdma_connect_worker [rpcrdma] is flushing !WQ_MEM_RECLAIM hns_roce_irq_workq:flush_work_handle [hns_roce_hw_v2] WARNING: CPU: 0 PID: 8250 at kernel/workqueue.c:2644 check_flush_dependency+0xe0/0x144 Call trace: check_flush_dependency+0xe0/0x144 start_flush_work.constprop.0+0x1d0/0x2f0 _flush_work.isra.0+0x40/0xb0 flush_work+0x14/0x30 hns_roce_v2_destroy_qp+0xac/0x1e0 [hns_roce_hw_v2] ib_destroy_qp_user+0x9c/0x2b4 rdma_destroy_qp+0x34/0xb0 rpcrdma_ep_destroy+0x28/0xcc [rpcrdma] rpcrdma_ep_put+0x74/0xb4 [rpcrdma] rpcrdma_xprt_disconnect+0x1d8/0x260 [rpcrdma] xprt_rdma_connect_worker+0xc0/0x120 [rpcrdma] process_one_work+0x1cc/0x4d0 worker_thread+0x154/0x414 kthread+0x104/0x144 ret_from_fork+0x10/0x18 Since QP destruction frees memory, this wq should have the WQ_MEM_RECLAIM.	2026-06-03	7.5	CVE-2026-46265
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: do WoW offloads only on primary link In case of multi-link connection, WCN7850 firmware crashes due to WoW offloads enabled on both primary and secondary links. Change to do it only on primary link to fix it. Tested-on: WCN7850 hw2.0 PCI WLAN.HMT.1.1.c5-00284-QCAHMTSWPL_V1.0_V2.0_SILICONZ-1	2026-06-03	7.8	CVE-2026-46271
Liquid Web / StellarWP--BookIt	Authentication Bypass Using an Alternate Path or Channel vulnerability in Liquid Web / StellarWP BookIt allows Password Recovery Exploitation. This issue affects BookIt: from n/a before 2.5.4.1.	2026-06-02	7.5	CVE-2026-40780
Liquid Web / StellarWP--GiveWP	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Liquid Web / StellarWP GiveWP allows DOM-Based XSS. This issue affects GiveWP: from n/a through 4.14.5.	2026-06-01	7.1	CVE-2026-42678
LMS Community--Lyrion Music Server	Lyrion Music Server 9.2.0 contains an unauthenticated stored cross-site scripting vulnerability in the log viewer that allows attackers to inject malicious scripts by exploiting unescaped template variables. Attackers can inject XSS payloads through search, lines, and path query parameters or by crafting values that get logged such as URLs, User-Agent headers, stream titles, or player names to execute arbitrary scripts in users' browsers.	2026-06-05	7.2	CVE-2026-50231
LMS Community--Lyrion Music Server	Lyrion Music Server 9.2.0 contains a stored cross-site scripting vulnerability that allows attackers to inject malicious scripts through media file metadata tags like GENRE, ARTIST, and ALBUM. Attackers can craft files with XSS payloads in metadata tags that execute in the web interface when users view track information or play files, enabling access to management functions and settings disclosure.	2026-06-05	7.2	CVE-2026-50232
LMS Community--Lyrion Music Server	Lyrion Music Server 9.2.0 contains a path traversal vulnerability that allows unauthenticated attackers to read arbitrary files by exploiting directory traversal in the web server context. Attackers can manipulate file path parameters to access sensitive files outside the intended directory structure.	2026-06-05	7.5	CVE-2026-50234
Logtivity Activity Logs--Activity Logs, User Activity Tracking, Multisite Activity Log from Logtivity	Insertion of Sensitive Information Into Sent Data vulnerability in Logtivity Activity Logs Activity Logs, User Activity Tracking, Multisite Activity Log from Logtivity allows Retrieve Embedded Sensitive Data. This issue affects Activity Logs, User Activity Tracking, Multisite Activity Log from Logtivity: from n/a through 3.3.6.	2026-06-01	7.5	CVE-2026-42673
masaakitana--Booking Package	The Booking Package plugin for WordPress is vulnerable to Privilege Escalation via Account Takeover in versions up to, and including, 1.7.16.	2026-06-06	7.2	CVE-2026-9851

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This is due to a missing capability check on the 'updateUser' branch of the package_app_action AJAX endpoint, where the handler only validates a nonce and the dispatcher invokes Schedule::updateUser() with the \$administrator argument hard-coded to 1, bypassing the only owner-restriction check inside that function and allowing the target user to be determined solely by attacker-supplied input passed directly to wp_update_user(). This makes it possible for authenticated attackers, with Editor-level access and above, to change the email address and password of any account, including Administrator accounts, resulting in a full site takeover.			
mazyarpanahi--openedmed	OpenMed before 1.5.2 contains a remote code execution vulnerability in the PII privacy-filter model loading path. The privacy-filter dispatcher used broad substring matching on the user-supplied model_name parameter, allowing a value such as attacker/foo-privacy-filter-bar to route through a path that loads Hugging Face models with trust_remote_code=True. An unauthenticated attacker can supply a malicious model repository containing custom Transformers code via auto_map in config.json or tokenizer_config.json, which is imported and executed with the privileges of the OpenMed service process.	2026-06-02	9.8	CVE-2026-47117
MBS--Single-A	An unauthenticated remote attacker can recover a default, hard coded password from a firmware image and thus gain full access to all affected devices.	2026-06-03	9.8	CVE-2026-35075
MBS--Single-A	The bac-scanresult method allows a remote attacker with user privileges to delete arbitrary local files due to insufficient validation of user-controlled input.	2026-06-03	8.1	CVE-2026-35076
MBS--Single-A	The ugw-delete-file method allows a remote attacker with user privileges to delete arbitrary local files due to insufficient validation of user-controlled input.	2026-06-03	8.1	CVE-2026-35077
MBS--Single-A	The ugw-logstop method allows a remote attacker with user privileges to delete arbitrary local files due to insufficient validation of user-controlled input.	2026-06-03	8.1	CVE-2026-35078
MBS--Single-A	The ugw-restore method allows a remote attacker with user privileges to delete arbitrary local files due to insufficient validation of user-controlled input.	2026-06-03	8.1	CVE-2026-35079
MBS--Single-A	The ugw-restoreinfo method allows a remote attacker with user privileges to delete arbitrary local files due to insufficient validation of user-controlled input.	2026-06-03	8.1	CVE-2026-35080
MBS--Single-A	The ugw-logstop method allows a remote attacker with user privileges to terminate arbitrary processes due to insufficient validation of user-supplied input.	2026-06-03	8.1	CVE-2026-35081
MBS--Single-A	The ugw-logread method allows a remote attacker with user privileges to access arbitrary local files due to insufficient validation of user-supplied input.	2026-06-03	8.8	CVE-2026-35082
MBS--Single-A	A remote attacker with user privileges can exploit a stack buffer overflow to gain full system access as root.	2026-06-03	8.8	CVE-2026-35083
MBS--Single-A	A remote attacker with user privileges can exploit a stack buffer overflow in dali-devconfig to gain full system access as root.	2026-06-03	8.8	CVE-2026-35084
MBS--Single-A	A remote attacker with user privileges can exploit a stack buffer overflow in gdv-serverconfig to gain full system access as root.	2026-06-03	8.8	CVE-2026-35085
mcmilk--7-Zip	7-Zip is a file archiver with a high compression ratio. Versions 26.00 and prior contain a heap buffer overflow vulnerability caused by an under-allocation in the NTFS compressed stream buffer (GetCuSize shift UB), potentially allowing attackers to cause arbitrary code execution or application crashes. ClnStream::GetCuSize() in the NTFS handler computes the compression-unit buffer size as (UInt32)1 << (BlockSizeLog + CompressionUnit), and a crafted image with ClusterSizeLog >= 28 and CompressionUnit == 4 drives the exponent to 32, which is undefined behavior and collapses on x86/x64 so _inBuf is allocated as 1 byte.	2026-06-05	8.8	CVE-2026-48095

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ReadStream_FALSE then writes up to 256 MB of attacker-controlled data into that 1-byte buffer in 64 KB iterations, and because the CInStream object sits only 304 bytes after _inBuf, its vtable pointer is overwritten and the next dispatched call achieves a vtable hijack. On 32-bit builds the overflow is unconditionally reached; on 64-bit it requires the parallel 8 GB _outBuf allocation to succeed, otherwise failing closed to denial of service. The NTFS handler is enabled by default in stock 7z.dll and, via signature-based fallback matching "NTFS " at offset 3, will open a crafted image regardless of file extension during extraction or testing. Version 26.01 fixes the issue.			
mdjm--MDJM Event Management	The MDJM Event Management plugin for WordPress is vulnerable to Arbitrary File Upload in all versions up to, and including, 1.7.8.3 via the mdjm_send_comm_email function. This is due to no file type, extension, or MIME type validation being performed on uploaded files. This makes it possible for authenticated attackers, with administrator-level access and above, to upload files that may be executable, which makes remote code execution possible.	2026-06-06	7.2	CVE-2026-7537
medplum--medplum	Medplum before 5.1.14 contains a server-side request forgery vulnerability in the subscription worker that allows authenticated users to perform unauthorized internal network requests by creating FHIR Subscription resources with arbitrary endpoint URLs. Attackers can point subscription endpoints at internal addresses such as cloud instance metadata services, internal databases, or container orchestration endpoints to exfiltrate IAM credentials and patient health records via the POST body containing full FHIR resource payloads.	2026-06-02	8.5	CVE-2026-49120
Microsoft--Azure HorizonDB	Authentication bypass by spoofing in Azure HorizonDB allows an unauthorized attacker to elevate privileges over a network.	2026-06-04	10	CVE-2026-48567
Microsoft--Microsoft 365 Copilot	Improper neutralization of special elements used in a command ('command injection') in Microsoft Copilot allows an authorized attacker to execute code over a network.	2026-06-04	7.7	CVE-2026-45497
Microsoft--Microsoft Exchange Online	Improper authorization in Microsoft Exchange Online allows an unauthorized attacker to disclose information over a network.	2026-06-04	9.1	CVE-2026-48579
Microsoft--Microsoft SharePoint Enterprise Server 2016	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-06-01	8	CVE-2026-47294
milamer--parse-nested-form-data	parse-nested-form-data is a tiny node module for parsing FormData by name into objects and arrays. Prior to version 1.0.1, parseFormData() walks bracket and dot-notation FormData field names into nested objects without filtering reserved property keys. A single FormData field whose name begins with __proto__, or contains .__proto__. mid-path, causes the parser to traverse onto Object.prototype and assign properties there, polluting the prototype chain of every plain object in the running process. This issue has been patched in version 1.0.1.	2026-06-01	8.2	CVE-2026-45302
Mobatek--Mobatek MobaXterm	Mobatek MobaXterm 12.1 contains a structured exception handling (SEH) based buffer overflow vulnerability in the username field of session files that allows remote attackers to execute arbitrary code. Attackers can craft a malicious MobaXterm sessions file with overflow data that triggers the vulnerability when imported and executed, enabling reverse shell execution with user privileges.	2026-06-04	9.8	CVE-2019-25741
moby--moby/v2/daemon	Moby is an open source container framework. In versions prior to 29.5.1 and in moby/moby v2 prior to v2.0.0-beta.14, when a compressed archive is uploaded to a container via 'PUT /containers/{id}/archive' or piped through 'docker cp -', the daemon resolves decompression binaries (such as 'xz' or 'unpigz') from the container's filesystem rather than the host's due to incorrect ordering of operations. A malicious container image containing a trojanized decompression binary can achieve arbitrary code	2026-06-05	7.2	CVE-2026-41567

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execution with full daemon privileges, including host root UID and unrestricted capabilities, when a user uploads a compressed (xz or gzip) archive into that container. This issue is fixed in Docker Engine 29.5.1 and moby/moby v2.0.0-beta.14. Workarounds include only running containers from trusted images, using authorization plugins to restrict access to the `PUT /containers/{id}/archive` endpoint, and avoiding piping compressed archives into containers created from untrusted images			
Mojoomla--School Management	Incorrect Privilege Assignment vulnerability in Mojoomla School Management allows Privilege Escalation. This issue affects School Management: from n/a through 93.2.0.	2026-06-03	8.8	CVE-2025-15656
Mojoomla--School Management	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mojoomla School Management allows SQL Injection. This issue affects School Management: from n/a through 93.2.0.	2026-06-03	7.6	CVE-2025-15655
Neterbit--NW-431F Router	Improper Authentication (Authentication Bypass) exists in Neterbit NW-431F Router 20241014-IR03 and before. The router uses a weak/predictable cookie value for authentication. By modifying the cookie value (e.g., setting it to "admin"), an attacker can bypass the authentication schema and gain unauthorized access to admin functionalities.	2026-06-04	9.8	CVE-2025-67446
Neterbit--NW-431F Router	The network diagnosis (ping) module in Neterbit NW-431F Router 20241014-IR03 and before is vulnerable to OS command injection. The application does not properly sanitize user input in the IP address field before passing it to the system's ping command. An attacker can inject arbitrary OS commands, which will be executed with the privileges of the web server.	2026-06-04	9.8	CVE-2025-67447
Neterbit--NW-431F Router	An issue in Neterbit NW-431F Router vNW-431F-20241014-IR03 allows a remote attacker to obtain sensitive information and execute arbitrary code via a crafted command to the at_command.asp interface	2026-06-04	8.2	CVE-2025-69755
Neterbit--NW-431F Router	The SMS module in Neterbit NW-431F Router 20241014-IR03 and before is vulnerable to stored XSS. The application does not properly sanitize user input in SMS messages before storing and displaying them. An attacker can send an SMS containing a malicious XSS payload, which will be executed in the context of the victim's browser when the message is viewed.	2026-06-04	7.1	CVE-2025-67448
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. From versions 0.3.0 to before 3.1.0, 5.0.0 to before 5.1.0, and 6.0.0 to before 6.4.0, a missing signature verification in User OIDC allowed a malicious ID4me authority to identify as any user. This issue has been patched in versions 3.1.0, 4.1.0, 5.1.0, 6.4.0 and 8.3.0.	2026-06-01	8.1	CVE-2026-45156
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 32.0.0 to before 32.0.9, and 33.0.0 to before 33.0.3, with the knowledge of other users' principal URL an attacker could possibly send a request to gain full access to their calendar. Therefore, the attacker must be an authenticated user. This is because of improper authorization controls in the backend of the calendar. If the attacker had access to the calendar, they would be able to view and modify it. It is recommended that the Nextcloud Server is upgraded to 33.0.3 or 32.0.9. It is recommended that the Nextcloud Enterprise Server is upgraded to 33.0.3, 32.0.9, 31.0.14.5, 30.0.17.9, 29.0.16.16, 28.0.14.17, 27.1.11.26, 26.0.13.26, 25.0.13.29, 24.0.12.34, 23.0.12.35, 22.2.10.39, or 21.0.9.23	2026-06-01	8.1	CVE-2026-45281
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. From versions 0.7.0 to before 0.7.7, 0.8.0 to before 0.8.10, 0.9.0 to before 0.9.8, and 1.0.0 to before 1.0.4, an authenticated attacker with access to the Tables app may be able to execute arbitrary up to 20 bytes long SQL queries, through a stored injection. With carefully crafted input it is possible to break out of the length limitation. The attacker could use this to extract information from the database, or modify data. This issue has been patched in versions 0.7.7, 0.8.10, 0.9.8, 1.0.4, and 2.0.0.	2026-06-01	8.2	CVE-2026-45545

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. From versions 0.9.0 to before 0.9.7, and 1.0.0 to before 1.0.2, a missing sanitization in the Tables app allowed a user with access to the tables app to perform a limited SQL injection in the ORDER BY statement of a query. Compared to normal SQL injections, the ORDER BY is limited to extracting a single bit of information per request or to make the database wait for a given time. This issue has been patched in versions 0.9.7 and 1.0.2.	2026-06-01	7.1	CVE-2026-45722
nextlevelbuilder-GoClaw	A vulnerability was found in nextlevelbuilder GoClaw up to 3.11.3. This impacts the function FsBridge.WriteFile of the file internal/sandbox/fsbridge.go of the component write_file Tool. Performing a manipulation results in os command injection. The attack is possible to be carried out remotely. The exploit has been made public and could be used. The pull request to fix this issue awaits acceptance.	2026-06-01	7.3	CVE-2026-10219
nextlevelbuilder-GoClaw	A security vulnerability has been detected in nextlevelbuilder GoClaw up to 3.11.3. This affects the function resolveAuth of the file internal/http/auth.go of the component Webhook Verification Handler. The manipulation leads to missing authentication. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The project tagged the reported issue as bug.	2026-06-02	7.3	CVE-2026-10617
NI--NI-PAL	Improper input validation in the NI-PAL kernel driver may allow a local authenticated user to cause a denial of service by triggering a crash due to a NULL pointer dereference. This vulnerability affects NI-PAL 26.3.0 and prior versions on Windows and Linux.	2026-06-02	7.1	CVE-2026-8035
NI--NI-PAL	Improper input validation in NI-PAL may allow a local authenticated user to access arbitrary system memory, potentially leading to privilege escalation. This vulnerability affects NI-PAL 26.3.0 and prior versions on Windows and Linux.	2026-06-02	7.1	CVE-2026-8036
Nicheoffice--All in One Video Downloader	All in One Video Downloader 1.2 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send requests to the admin interface with UNION-based SQL injection payloads in the id parameter to extract sensitive database information including usernames, databases, and version details.	2026-06-04	8.2	CVE-2019-25726
NousResearch--hermes-agent	A vulnerability was determined in NousResearch hermes-agent up to 2026.4.30. Affected is the function _serve_plugin_skill/skill_view of the file tools/skills_tool.py. Executing a manipulation can lead to injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-01	7.3	CVE-2026-10220
NousResearch--hermes-agent	A vulnerability was identified in NousResearch hermes-agent up to 0.12.0. Affected by this vulnerability is the function _compress_context of the file run_agent.py. The manipulation leads to injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-01	7.3	CVE-2026-10221
nsauditor--NetShareWatcher	NetShareWatcher 1.5.8.0 contains a structured exception handler buffer overflow vulnerability that allows local attackers to execute arbitrary code by supplying malicious input. Attackers can craft a payload with overwritten SEH and NSEH pointers through the Restrictions custom filter field to trigger code execution when the Find function is invoked.	2026-06-04	8.4	CVE-2019-25733
NVIDIA--NVTabular	NVIDIA NVTabular contains a vulnerability where an attacker could cause improper deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, data tampering and information disclosure.	2026-06-02	7.8	CVE-2026-24221
NVIDIA--NVTabular	NVIDIA NVTabular contains a vulnerability where an attacker could cause improper deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, data tampering, and information disclosure.	2026-06-02	7.8	CVE-2026-24237

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nvm-sh--nvm	nvm (Node Version Manager) through 0.40.4 executes arbitrary commands from version strings supplied by the configured Node.js/io.js mirror. Commands such as `nvm install` read the available versions from the mirror's index.tab and use the selected version, without sanitization, to build download URLs and shell/awk commands. Two sinks are affected by the same untrusted input: nvm_download() built a curl/wget command string and ran it with `eval`, so a version field containing command substitution (for example \$(id)) was executed by the local shell; and nvm_get_checksum() interpolated the version-derived download slug into an awk program, so a crafted version could execute arbitrary commands via awk's system(). An attacker who controls the configured mirror, supplies mirror content to a user or CI on a non-default mirror, or machine-in-the-middle a non-TLS mirror can run arbitrary commands with the privileges of the user running nvm. The default mirror (https://nodejs.org over TLS) is not affected. Fixed on master (pending the next tagged release) by passing every argument as a literal argv element instead of using eval, by passing the value to awk as data via -v instead of interpolating it into the program, and by rejecting any version outside the Node.js/io.js version grammar before it is used.	2026-06-04	7.5	CVE-2026-10796
OP-TEE--optee_os	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 3.16.0 and prior to 4.11.0, a user-after-free (UAF) race condition exists in the shared memory teardown logic of FF-A within OP-TEE SPMC/SP flows. This only applies when OP-TEE is configured as an SPMC for S-EL0 SPs, that is, with `CFG_SECURE_PARTITION=y`. The function `sp_mem_remove()`, responsible for freeing entries in `smem->receivers` and `smem->regions`, fails to acquire the global `sp_mem_lock` before performing the `free()` operations. Concurrently, other code paths, such as `sp_mem_get_receiver()`, iterate over these same lists without holding a lock, or, like `sp_mem_is_shared()`, iterate while holding the lock but are not serialized against the unprotected `free()` in `sp_mem_remove()`. This creates a cross-thread race where a thread iterating the list can acquire a pointer to an entry (e.g., `struct sp_mem_map_region` or `struct sp_mem_receiver`), and then another thread calls `sp_mem_remove()`, freeing the object. When the first thread resumes and dereferences the pointer, it results in a Use-After-Free vulnerability. Version 4.11.0 fixes the issue.	2026-06-03	7.8	CVE-2026-40290
open-telemetry--opentelemetry-ebpf-instrumentation	OpenTelemetry eBPF Instrumentation provides eBPF instrumentation based on the OpenTelemetry standard. Prior to version 0.9.0, the Postgres protocol parser assumes BIND message payloads contain a valid NUL-terminated portal name. A crafted empty or unterminated payload can make OBI slice beyond the end of the captured buffer and panic. This issue has been patched in version 0.9.0.	2026-06-02	7.5	CVE-2026-45678
open-telemetry--opentelemetry-ebpf-instrumentation	OpenTelemetry eBPF Instrumentation provides eBPF instrumentation based on the OpenTelemetry standard. From version 0.1.0 to before version 0.9.0, malformed MongoDB wire messages can trigger uncaught panics in the MongoDB TCP parser, allowing a remote unauthenticated attacker to crash the telemetry agent and cause a denial of service. The parser operates on raw attacker-controlled network payloads before the input is fully validated, so a single crafted message can terminate telemetry collection for the affected process or node. This issue has been patched in version 0.9.0.	2026-06-02	7.5	CVE-2026-45685
open-telemetry--opentelemetry-ebpf-instrumentation	OpenTelemetry eBPF Instrumentation provides eBPF instrumentation based on the OpenTelemetry standard. From version 0.7.0 to before version 0.9.0, a remotely reachable integer overflow in OBI's memcached text protocol parser can crash the OBI process and cause denial of service. When parsing memcached storage commands such as set, add, replace, append, prepend, or cas, OBI accepts extremely large <bytes> values and	2026-06-02	7.5	CVE-2026-45686

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	adds the payload delimiter length without checking for overflow. A crafted request with <bytes> set to math.MaxInt or math.MaxInt-1 causes the computed payload length to wrap negative and triggers a runtime panic in LargeBufferReader.Peek. This issue has been patched in version 0.9.0.			
OpenStack--Mistral	OpenStack Mistral through 22.0.0 allows Arbitrary Remote Code Execution when the API is exposed. There are endpoints that allow code execution, which can lead to exfiltration of service credentials.	2026-06-04	9.9	CVE-2026-41283
Os-nexus--QuantaStor	OSNexus QuantaStor SDS Manager is vulnerable to SQL injection in the login endpoint. The username field is not properly sanitized before being incorporated into a SQL query, allowing an unauthenticated remote attacker to bypass authentication and log in as an administrator without supplying a valid password.	2026-06-04	9.8	CVE-2026-10880
OTRS AG--OTRS	An improper Input Validation vulnerability in OTRS or ((OTRS)) Community Edition database layer module allows an unauthenticated SQL injection which can lead to an authentication bypass. This issue only affects the system if the MySQL/MariaDB server is configured with the NO_BACKSLASH_ESCAPES SQL mode. This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.4.X * ((OTRS)) Community Edition: 6.0.x Products based on the ((OTRS)) Community Edition also very likely to be affected	2026-06-01	9.1	CVE-2026-48188
OTRS AG--OTRS	An improper neutralization of user-controllable input in OTRS or ((OTRS)) Community Edition ticket handling allows authenticated attackers to perform reflected cross-site scripting (XSS) attacks via crafted request parameters associated with ticket actions. By injecting malicious JavaScript into manipulated request URLs, attackers can execute arbitrary script code in the context of an authenticated agent session when the crafted link is opened. This issue affects OTRS: * 7.0.x Please note that ((OTRS)) Community Edition 6.x and before are vulnerable. Products based on the ((OTRS)) Community Edition also very likely to be affected	2026-06-01	7.1	CVE-2026-48209
Paroiciel--Paroiciel	Paroiciel 11.20 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the tRecIdListe parameter. Attackers can send GET requests to the trec.php endpoint with crafted SQL payloads to extract database information including table and column names.	2026-06-01	8.2	CVE-2018-25428
Paroiciel--Paroiciel	Paroiciel 11.20 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the zProIdPro parameter. Attackers can send GET requests to zpro.php with crafted SQL payloads in the zProIdPro parameter to extract sensitive database information including usernames, databases, and version details.	2026-06-01	7.1	CVE-2018-25429
Paroiciel--Paroiciel	Paroiciel 11.20 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the eGeqIdEquipe parameter. Attackers can send GET requests to the egeq.php endpoint with crafted SQL payloads to extract sensitive database information including version details and other data.	2026-06-01	7.1	CVE-2018-25430
perfree--go-fastdfs-web	A flaw has been found in perfree go-fastdfs-web up to 1.3.7. Affected is the function checkServer of the file /install/checkServer of the component Installation Endpoint. Executing a manipulation can lead to server-side request forgery. The attack can be executed remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-06	7.3	CVE-2026-11437
Phoenix Contact--CHARX SEC-3150	It is possible for an unauthenticated adjacent attacker to download log files of the controller, which may disclose some restricted information.	2026-06-03	7.5	CVE-2026-41032
php-censor--php-censor	A vulnerability was found in php-censor up to 2.1.6. This affects an unknown function of the file src/Model/Build/GitBuild.php of the component Webhook Endpoint. Performing a manipulation of the argument commitId results in os command injection. The attack can be	2026-06-01	7.3	CVE-2026-10273

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	initiated remotely. The exploit has been made public and could be used. The patch is named cd68d102601320bd319d590b75f7652e66f0685f. It is recommended to apply a patch to fix this issue.			
Pixastudio--Pixa Bank	Pixa Bank 2.0 contains an SQL injection vulnerability that allows unauthenticated attackers to extract sensitive data by injecting SQL code into the 'rib' parameter. Attackers can send POST requests to the agence-ajax.php endpoint with UNION-based SQL payloads to retrieve user information including names, email addresses, and phone numbers from the database.	2026-06-01	8.2	CVE-2026-49491
plugcrux--Integration for Freshsales Contact Form 7, WPForms, Elementor, Gravity Forms and More	The Integration for Freshsales - Contact Form 7, WPForms, Elementor, Gravity Forms and More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Form Submission Data in all versions up to, and including, 1.0.15 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The injected payload only executes when a CRM API call fails for the submitted form and an administrator subsequently views the error log details modal in the WordPress admin panel.	2026-06-06	7.2	CVE-2026-8901
Progress Software--LoadMaster	OS Command Injection Remote Code Execution Vulnerability in API in Progress ADC Products allows an un-authenticated attacker to execute arbitrary commands on the LoadMaster appliance by exploiting unsanitized input in multiple command endpoints	2026-06-04	9.6	CVE-2026-8037
Progress Software--Sitefinity	CWEâ€‘522: Insufficiently Protected Credentials in web services in Progress Sitefinity version from 14.0.7700 to 14.4.8152, and 15.0.8200 to 15.0.8234, and 15.1.8300 to 15.1.8335, 15.2.8400 to 15.2.8441, 15.3.8500 to 15.3.8531, and 15.4.8600 to 15.4.8630 allows a remote unauthenticated attacker to obtain plain-text credentials used connect to Sitefinity Insight service. Successful exploitation requires active integration with Sitefinity Insight and non-default site configuration.	2026-06-02	10	CVE-2026-7312
Progress Software--Sitefinity	CWE-284: Improper Access Control in web services in Progress Sitefinity 15.4.8623 before 15.4.8630 allows a remote unauthenticated attacker to access content that should be restricted, resulting in full compromise of confidentiality, integrity, and availability of affected installations.	2026-06-02	9.8	CVE-2026-7198
Progress Software--Sitefinity	CWE-20: Improper Input Validation in web services in Progress Sitefinity 14.1.x through 14.3.x, 14.4.x before 14.4.8152, 15.0.x before 15.0.8234, 15.1.x before 15.1.8335, 15.2.x before 15.2.8441, 15.3.x before 15.3.8531, and 15.4.x before 15.4.8630 allows a remote unauthenticated attacker to compromise the integrity and confidentiality of user accounts. Successful exploitation requires user interaction and a non-default site configuration.	2026-06-02	8.8	CVE-2026-7195
Progress Software--Sitefinity	CWE-639: Authorization Bypass Through User-Controlled Key in web services in Progress Sitefinity 15.2.x before 15.2.8441, 15.3.x before 15.3.8531, and 15.4.x before 15.4.8630 allows a remote authenticated attacker to modify account properties of other users, potentially leading to account compromise. Successful exploitation requires knowledge of values that are not generally exposed to low-privileged users.	2026-06-02	8.8	CVE-2026-7201
Progress Software--Sitefinity	CWEâ€‘522: Insufficiently Protected Credentials in web services in Progress Sitefinity version from 8.0.5700 to 13.3.7652 allows a remote authenticated attacker to obtain plain-text credentials used connect to Sitefinity Insight service. Successful exploitation requires active integration with Sitefinity Insight, non-default site configuration and valid back-end authorization.	2026-06-02	8.7	CVE-2026-7313
Qualcomm, Inc.--Snapdragon	Cryptographic Issue while processing a specific partition which allows unauthorized write access to load a customized bootloader.	2026-06-01	8.2	CVE-2026-24088
Qualcomm, Inc.--Snapdragon	Memory corruption while using Strongbox due to missing bounds check.	2026-06-01	8.8	CVE-2026-25276
Qualcomm, Inc.--Snapdragon	Memory corruption while using Strongbox due to buffer overflow.	2026-06-01	8.8	CVE-2026-25277
Qualcomm, Inc.--Snapdragon	Memory Corruption when running a memory copy operation due to invalid writes caused by a null pointer.	2026-06-01	7.8	CVE-2025-59604

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Qualcomm, Inc.-- Snapdragon	Memory Corruption when processing device identifier strings that exceed the expected maximum length.	2026-06-01	7.8	CVE-2025-59605
Qualcomm, Inc.-- Snapdragon	Memory Corruption when writing to invalid memory locations occurs due to heap memory exhaustion during secure data initialization.	2026-06-01	7.8	CVE-2025-59606
Qualcomm, Inc.-- Snapdragon	Memory Corruption when processing display command line information due to improper initialization of a variable.	2026-06-01	7.2	CVE-2026-24085
Qualcomm, Inc.-- Snapdragon	Memory corruption while processing fastboot OEM commands.	2026-06-01	7.2	CVE-2026-24087
Qualcomm, Inc.-- Snapdragon	Memory corruption while processing fastboot commands with invalid input.	2026-06-01	7.2	CVE-2026-24089
Qualcomm, Inc.-- Snapdragon	Cryptographic issue while processing partition table entries allows unauthorized modification of boot flow.	2026-06-01	7.1	CVE-2026-24090
Qualcomm, Inc.-- Snapdragon	Memory corruption while processing fastboot commands with improperly formatted input.	2026-06-01	7.2	CVE-2026-24091
Qualcomm, Inc.-- Snapdragon	Memory Corruption when processing fastboot commands to set display mode.	2026-06-01	7.2	CVE-2026-24092
Qualcomm, Inc.-- Snapdragon	Memory corruption while processing IOCTL calls for escape operations.	2026-06-01	7.8	CVE-2026-25258
Qualcomm, Inc.-- Snapdragon	Memory corruption while processing multiple IOCTL command for escape operations.	2026-06-01	7.8	CVE-2026-25259
Qualcomm, Inc.-- Snapdragon	Memory Corruption when accessing shared buffers without validation of concurrent user-mode input modifications.	2026-06-01	7.8	CVE-2026-25260
raisulislamg4-- student_management_system_by_php	A vulnerability was detected in raisulislamg4 student_management_system_by_php up to 310d950e09013d5133c6b9210aff9444382d16d1. This issue affects some unknown processing of the file login_check.php of the component Login. Performing a manipulation of the argument Username results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	7.3	CVE-2026-10225
raisulislamg4-- student_management_system_by_php	A flaw has been found in raisulislamg4 student_management_system_by_php up to 310d950e09013d5133c6b9210aff9444382d16d1. Impacted is an unknown function of the file delete.php. Executing a manipulation of the argument user_id/course_id/teacher_id/student_id/application_id can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	7.3	CVE-2026-10226
raisulislamg4-- student_management_system_by_php	A vulnerability has been found in raisulislamg4 student_management_system_by_php up to 310d950e09013d5133c6b9210aff9444382d16d1. The affected element is an unknown function of the file add_user_check.php of the component User Creation Handler. The manipulation of the argument role leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	7.3	CVE-2026-10227
Red Hat--Builds for Red Hat OpenShift	A flaw was found in the OpenShift Pipelines operator. The tekton-scheduler-rolebinding ClusterRoleBinding grants the system:authenticated group write access to Kueue and cert-manager custom resources via the tekton-scheduler-role ClusterRole. When Kueue or cert-manager CRDs are present on the cluster, any authenticated user can disrupt workload scheduling, tamper with scheduling priorities, delete other tenants'	2026-06-04	9.6	CVE-2026-10840

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Workload objects, or induce cert-manager to overwrite TLS Secrets including the default ingress controller certificate.			
Red Hat--Red Hat Ansible Automation Platform 2	A flaw was found in ansible-core. The ansible-galaxy role install command processes dependency specifications from a role's meta/requirements.yml file. Due to improper neutralization of argument delimiters, a malicious role author can inject arbitrary git configuration flags through the src field. This allows arbitrary code execution on the machine of a user who installs the role via ansible-galaxy role install.	2026-06-05	7.8	CVE-2026-11332
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in Poppler's Splash backend. A remote attacker could exploit this vulnerability by crafting a malicious PDF file that, when rendered, triggers an integer overflow in the `tilingPatternFill` function. This overflow leads to an undersized heap memory allocation, allowing a subsequent out-of-bounds write. Successful exploitation could result in arbitrary code execution, information disclosure, or denial of service within the context of the application processing the PDF.	2026-06-01	7.8	CVE-2026-10118
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in rrdcached, a component of rrdtool. A local attacker with access to a rrdcached socket can exploit a stack-based buffer overflow by sending an oversized CREATE request. This vulnerability can lead to a denial of service by crashing the daemon or potentially allow for arbitrary code execution, impacting the integrity and confidentiality of data.	2026-06-01	7.8	CVE-2026-43958
Red Hat--Red Hat Enterprise Linux 10	A stack-based buffer overflow flaw was found in the X.Org X server and Xwayland. A mismatch between the X server and the libXfont2 library's maximum font name length can cause a stack buffer overflow during font alias resolution. The server allocates a 256 byte stack buffer but libXfont2's alias target name length is 1024 bytes. A font alias name between 257 and 1023 bytes causes the X server to copy that name into the undersized stack buffer without further checks. This may be used to crash the server, or for privilege escalation if the X server runs as root.	2026-06-05	7.8	CVE-2026-50256
Red Hat--Red Hat Enterprise Linux 10	A use-after-free flaw was found in the X.Org X server and Xwayland in miSyncDestroyFence(). A client that sets up multiple fence triggers can trigger a use-after-free function pointer call. An attacker would connect to the X server to set up a fence and await that fence, then a second X connection destroys the fence, causing the use-after-free. This may be used to crash the server, or for privilege escalation if the X server runs as root.	2026-06-05	7.8	CVE-2026-50257
Red Hat--Red Hat Enterprise Linux 10	A stack-based buffer overflow flaw was found in the X.Org X server and Xwayland. The X server has multiple stack buffers sized XkbMaxShiftLevel * XkbNumKbdGroups but CheckKeyTypes() does not verify or clamp non-canonical key types to XkbMaxShiftLevel. A client can change key types to excessive shift levels and trigger stack overflows. This is caused by an incomplete fix of CVE-2025-26597. This may be used to crash the server, or for privilege escalation if the X server runs as root.	2026-06-05	7.8	CVE-2026-50258
Red Hat--Red Hat Enterprise Linux 10	A stack-based buffer overflow flaw was found in the X.Org X server and Xwayland. _XkbSetMapChecks() declares a fixed-size stack buffer mapWidths[256] indexed by key type index. The helper function CheckKeyTypes() writes to this buffer at a client-controlled offset, allowing a stack buffer overflow. This may be used to crash the server, or for privilege escalation if the X server runs as root.	2026-06-05	7.8	CVE-2026-50259
Red Hat--Red Hat Enterprise Linux 10	A use-after-free flaw was found in the X.Org X server and Xwayland in FreeCounter(). A client that sets up multiple SyncCounters and awaits on those triggers can trigger a use-after-free when destroying those counters via a second client connection. This may be used to crash the server, or for privilege escalation if the X server runs as root.	2026-06-05	7.8	CVE-2026-50260
Red Hat--Red Hat Enterprise Linux 10	A use-after-free flaw was found in the X.Org X server and Xwayland in SyncChangeCounter(). A client that sets up multiple SyncCounters can trigger a use-after-free when destroying those counters via a second client connection while changing those counters. This may be used to crash the server, or for privilege escalation if the X server runs as root.	2026-06-05	7.8	CVE-2026-50261

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat Enterprise Linux 10	An out-of-bounds write flaw was found in the X.Org X server and Xwayland in <code>DRI2GetBuffers/DRI2GetBuffersWithFormat</code> . A client that requests multiple <code>DRI2BufferBackLeft</code> attachments and one <code>DRI2BufferFrontLeft</code> can trigger an out-of-bounds heap write. This may be used to crash the server, or for privilege escalation if the X server runs as root.	2026-06-05	7.8	CVE-2026-50264
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in <code>libinput</code> . A local attacker with access to <code>/dev/uinput</code> can inject arbitrary <code>udev</code> properties through the <code>libinput-device-group</code> helper. This injection can lead to root code execution, for example, by exploiting <code>REMOVE_CMD</code> properties that are executed when a device is removed. This vulnerability allows an attacker to gain elevated privileges on the system.	2026-06-05	7	CVE-2026-50265
Red Hat--Red Hat OpenShift Container Platform 4	The Route OpenShift resource allows to define routes to make pods reachable at a subdomain through HAProxy. It was found that the checks performed on the <code>spec.path</code> YAML stanza in a Route document was insufficient and could allow a controlled injection of the HAProxy configuration.	2026-06-02	8.8	CVE-2026-1784
Red Hat--Red Hat OpenShift Container Platform 4	A flaw was found in the OpenShift Cloud Credential Operator Mint-mode IAM policies for AWS. Operator credentials are provisioned with account-wide scope for destructive actions rather than being restricted to cluster-owned resources, enabling cross-scope impact after credential compromise.	2026-06-04	7.2	CVE-2026-10843
remix-run--react-router	React Router is a router for React. In versions 7.7.0 through 7.13.1, when using React Router's unstable React Server Components (RSC) APIs, there is a potential client-side Cross-Site Scripting (XSS) vulnerability in the RSC redirect handling if redirects come from untrusted sources. This does not impact applications that are not using the unstable RSC APIs in React Router. This is patched in version 7.13.2.	2026-06-02	8	CVE-2026-33245
remix-run--react-router	React Router is a router for React. In versions 7.0.0 through 7.14.1, when using Framework Mode, a combination of steps could potentially allow unauthorized remote code execution (RCE) through external requests. This attack requires the application code to have an existing prototype pollution vulnerability, which can then be leveraged in a 2-step attack where the second step triggers unauthorized RCE on the remote server. This does not impact applications using Declarative Mode (<code><BrowserRouter></code>) or Data Mode (<code>createBrowserRouter/<RouterProvider></code>). This is patched in version 7.14.2.	2026-06-02	8.1	CVE-2026-42211
remix-run--react-router	React Router is a router for React. In versions 7.7.0 through 7.13.1, when using React Router's unstable React Server Components (RSC) APIs, there is a potential client-side Cross-Site Scripting (XSS) vulnerability in the RSC redirect handling if redirects come from untrusted sources. This does not impact applications that are not using the unstable RSC APIs in React Router. This is patched in version 7.13.2.	2026-06-02	7.5	CVE-2026-34077
remix-run--react-router	React Router is a router for React. In versions 7.0.0 through 7.14.x of <code>react-router</code> and versions 2.10.0 through 2.17.4 of <code>@remix-run/server-runtime</code> , certain crafted requests can consume disproportionate server resources via unbounded path expansion in the <code>__manifest</code> endpoint, resulting in response time degradation and/or service unavailability for end users. This affects React Router Framework Mode applications as well as Remix applications. This does not impact applications using Declarative Mode (<code><BrowserRouter></code>) or Data Mode (<code>createBrowserRouter/<RouterProvider></code>). This is patched in <code>react-router</code> version 7.15.0 and <code>@remix-run/server-runtime</code> version 2.17.5.	2026-06-02	7.5	CVE-2026-42342
Riello UPS--NetMan 204	NetMan 204 contains a hard-coded backdoor account with the username and password 'eurek' that grants administrative access. A remote, unauthenticated attacker can authenticate through the <code>cgi-bin/login.cgi</code> endpoint (for example <code>/cgi-bin/login.cgi?username=eurek&password=eurek</code> , which due to lax parameter validation can be shortened to <code>/cgi-</code>	2026-06-05	9.8	CVE-2025-71317

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bin/login.cgi?username=eurek%20eurek) to obtain administrator privileges, allowing them to alter device configuration, enable the telnet/SSH services, and reset local user credentials.			
Riello UPS-- NetMan 204	NetMan 204 fails to enforce authentication on its administrative pages and command endpoints. A remote, unauthenticated attacker can directly request administrative pages (such as administration.html, administration-commands.html, and configuration.html) to disclose sensitive information including LDAP configuration and active user details, and can invoke privileged UPS control commands - including shutdown, reboot, switch-on-bypass, and battery test - without supplying any credentials.	2026-06-05	9.8	CVE-2025-71318
Rocketgenius Inc.--Gravity Forms	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Rocketgenius Inc. Gravity Forms allows Path Traversal. This issue affects Gravity Forms: from n/a through 2.10.0.1.	2026-06-01	9.6	CVE-2026-48866
ROCm--aiter	AI Tensor Engine for ROCm (AITER) through 0.1.14 contains an unauthenticated remote code execution vulnerability in the MessageQueue.recv() function within shm_broadcast.py that allows unauthenticated remote attackers to execute arbitrary code by sending a malicious pickle payload to a ZMQ SUB socket with no authentication, HMAC, or format validation. Attackers who can reach the writer XPUB endpoint on the cluster network or supply a forged Handle with an attacker-controlled remote_subscribe_addr can deliver a crafted pickle payload that executes arbitrary code simultaneously as the inference worker process on every remote reader worker.	2026-06-01	8.1	CVE-2026-49121
rxi--microtar	microtar through 0.1.0 contains a stack-based buffer overflow vulnerability in the raw_to_header() function in src/microtar.c that allows attackers to corrupt adjacent stack memory by supplying a crafted TAR archive with non-null-terminated name or linkname fields. The function uses strcpy() to copy 100-byte ustar format fields that lack null terminators, causing writes of up to 355 bytes into a 100-byte destination buffer when mtar_open(), mtar_find(), or mtar_read_header() process attacker-supplied TAR archives.	2026-06-01	8.8	CVE-2026-43623
sayan365-- student- management- system	A vulnerability was detected in sayan365 student-management-system up to 7f3c9ce7d410332335c2affac93a385485051800. This impacts an unknown function. The manipulation results in improper authentication. The attack can be executed remotely. The exploit is now public and may be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. Multiple endpoints are affected. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-02	7.3	CVE-2026-10619
Screets--Live Chat Unlimited	Live Chat Unlimited 2.8.3 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts through the chat input field. Attackers can submit payloads containing script tags and event handlers that execute in the admin area, enabling cookie theft or forced redirects to malicious websites.	2026-06-04	7.2	CVE-2019-25737
Seagull Software, LLC.--BarTender 2010	Seagull Software BarTender 2010, 2016, and 2019 contain an unauthenticated remote code execution vulnerability in the .NET Remoting service exposed on TCP port 7375 via BtSystem.Service.exe. The service registers an unauthenticated singleton endpoint - BarTenderSystem for BarTender 2016 <= R9, and DataServiceSingleton for BarTender 2019 <= R10 - configured with BinaryServerFormatterSinkProvider and TypeFilterLevel set to Full. An unauthenticated remote attacker can exploit .NET Remoting object unmarshalling to read or write arbitrary files on the server using the .NET WebClient class, or coerce NTLMv2 authentication by supplying a UNC path to an attacker-controlled server, enabling sensitive credential disclosure, remote code execution, or lateral movement depending on service account privileges and network environment. The service runs in the context of NT AUTHORITY\SYSTEM.	2026-06-04	9.8	CVE-2026-25550

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Seagull Software, LLC--BarTender 2021	Seagull Software BarTender 2021 R1 through 12.0.1 contains an insecure deserialization vulnerability that allows low-privileged local users to escalate privileges. The DataServiceSingleton .NET Remoting endpoint is bound to localhost on TCP port 7375 via BtSystem.Service.exe, limiting the attack surface to local access only. The endpoint is configured with BinaryServerFormatterSinkProvider and TypeFilterLevel set to Full. A low-privileged local attacker can send YSoSerial.NET-generated BinaryFormatter payloads to the localhost-bound endpoint to achieve code execution as NT AUTHORITY\SYSTEM.	2026-06-04	7.8	CVE-2026-25551
Select-Themes--WaveRide	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Select-Themes WaveRide allows PHP Local File Inclusion. This issue affects WaveRide: from n/a through 1.4.	2026-06-02	8.1	CVE-2026-39553
Sergey--AIWU	Incorrect Privilege Assignment vulnerability in Sergey AIWU allows Privilege Escalation. This issue affects AIWU: from n/a through 1.4.17.	2026-06-01	9.8	CVE-2026-48879
ShapedPlugin, LLC--Product Slider Pro for WooCommerce	Improper Validation of Specified Quantity in Input vulnerability in ShapedPlugin, LLC Product Slider Pro for WooCommerce allows Malicious Software Implanted. This issue affects Product Slider Pro for WooCommerce: from n/a before 3.5.3. No patched version is available - the vendor has applied a fix to an existing release without publishing a new version. While the patch provided by the vendor is valid, releasing it under the existing version number leaves users unable to reliably determine whether they are running a patched or vulnerable installation. As a result, we treat this as an unpatched version.	2026-06-05	10	CVE-2026-49777
shd101wyy--Markdown Preview Enhanced	Markdown Preview Enhanced before 0.8.28 opens external files and links from the preview through a shell and does not validate untrusted inputs taken from the markdown document - the diagram filename attribute, imported file paths, and the latex_engine code-chunk attribute. On Windows, a crafted markdown document can inject operating system commands that execute when the document is previewed. Fixed in 0.8.28 by passing these inputs as literal arguments instead of through a shell and validating them before use.	2026-06-05	8.8	CVE-2026-49492
shd101wyy--Markdown Preview Enhanced	Markdown Preview Enhanced before 0.8.28 parses Bitfield fenced code blocks with interpretJS(), which evaluates the block content as code via vm.runInNewContext(), allowing arbitrary code execution. A crafted markdown document containing a malicious bitfield code block executes attacker-controlled code on the server side when the document is rendered or exported. Fixed in 0.8.28 by parsing bitfield register definitions with JSON5.parse(), since they are purely data.	2026-06-05	8.8	CVE-2026-49493
shd101wyy--Markdown Preview Enhanced	Markdown Preview Enhanced before 0.8.28 parses WaveDrom diagrams by evaluating untrusted markdown content with eval(), allowing arbitrary JavaScript execution. The flaw affects every render path - the live preview (window.eval) and presentation mode plus HTML export (the bundled WaveDrom.ProcessAll()/eva() helpers) - and can also be triggered through a <script type="WaveDrom"> element injected via raw HTML in markdown. When a victim previews or exports a crafted markdown document, an attacker can execute arbitrary code, leading to arbitrary file write. Fixed in 0.8.28 by parsing with JSON5.parse() and sanitizing WaveDrom data scripts to inert strict JSON.	2026-06-05	8.8	CVE-2026-50733
shd101wyy--Markdown Preview Enhanced	Markdown Preview Enhanced 0.8.x with crossnote engine 0.9.28 contains a code injection vulnerability in the WaveDrom rendering pipeline that allows attackers to execute arbitrary JavaScript by embedding malicious content in a wavedrom fenced code block within a crafted Markdown document. Attackers can exploit the unsanitized passing of wavedrom block content to window.eval() in the VS Code webview context to abuse the extension's message passing and invoke arbitrary file writes on the local filesystem.	2026-06-05	7.1	CVE-2026-11422
Shibby--Tomato	A flaw has been found in Shibby Tomato 1.28.0000. This affects the function start_dhcpd of the file /sbin/rc of the component Web UI. This	2026-06-04	7.2	CVE-2026-10870

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	manipulation causes os command injection. It is possible to initiate the attack remotely. The exploit has been published and may be used. This project is superseded by FreshTomato.			
Shibby--Tomato	A vulnerability has been found in Shibby Tomato 1.28.0000. This vulnerability affects the function start_6rd_tunnel of the file /sbin/rc of the component Web UI. Such manipulation of the argument ipv6_6rd_borderrelay leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This project is superseded by FreshTomato.	2026-06-04	7.2	CVE-2026-10871
Shibby--Tomato	A vulnerability was found in Shibby Tomato 1.28.0000. This issue affects the function start_vpnserver of the file /sbin/rc of the component Web UI. Performing a manipulation results in os command injection. The attack can be initiated remotely. The exploit has been made public and could be used. This project is superseded by FreshTomato.	2026-06-04	7.2	CVE-2026-10872
Shibby--Tomato	A vulnerability was determined in Shibby Tomato 1.28.0000. Impacted is the function rstats_path of the file /bin/rstats of the component Web UI. Executing a manipulation can lead to os command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. This project is superseded by FreshTomato.	2026-06-04	7.2	CVE-2026-10873
simcy_creative--PDF Signer	PDF Signer 3.0 contains a server-side template injection vulnerability that allows unauthenticated attackers to execute arbitrary code by injecting PHP commands through the CSRF-TOKEN cookie parameter. Attackers can craft malicious cookie values containing template injection payloads like shell_exec() to execute system commands and retrieve sensitive information from the server.	2026-06-04	9.8	CVE-2019-25729
smartypants--SP Project & Document Manager	The SP Project & Document Manager plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the view_file function in all versions up to, and including, 4.71. This makes it possible for unauthenticated attackers to read file metadata and obtain download links for arbitrary files stored inside project folders on the server, which can contain sensitive information. The authorization gate uses a negated nonce check OR-chained with permission checks, meaning a missing or invalid nonce causes the entire condition to evaluate to true and bypass all preceding capability and ownership checks. The secondary fallback check only denies access for root-level files (pid == 0), leaving all files stored inside project folders fully exposed to unauthenticated users who supply only a valid file ID in a POST request to admin-ajax.php.	2026-06-04	7.5	CVE-2026-10737
SMCI--AS-2115HS-TNR	There is a vulnerability in the Supermicro BMC SMTP service at Supermicro AS-2115HS-TNR. An attacker may obtain administrator privileges and inject specially crafted characters into the SMTP service configuration. This may cause the underlying system to execute unintended commands during process invocation. Potential impact includes denial-of-service attacks, arbitrary code execution, or permanent compromise of the controller.	2026-06-04	7.2	CVE-2026-3820
SolarWinds--Serv-U	SolarWinds Serv-U is susceptible to specially crafted POST requests that crash the Serv-U service without authentication using Content-Encoding: deflate. Mitigation steps are provided to secure customer environments in the SolarWinds Trust Center if you are unable to deploy the update	2026-06-04	7.5	CVE-2026-28318
SolarWinds--Web Help Desk	SolarWinds Web Help Desk is found to be affected by a denial-of-service vulnerability, which when exploited, could cause the Web Help Desk server to crash due to insufficient memory.	2026-06-02	8.2	CVE-2026-28299
SourceCodester--Computer Repair Shop Management System	A vulnerability was found in SourceCodester Computer Repair Shop Management System up to 1.0. Affected is an unknown function of the file /admin/products/manage_product.php. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	2026-06-01	7.3	CVE-2026-10263
SourceCodester--Online Food Ordering System	A vulnerability was detected in SourceCodester Online Food Ordering System 2.0. Affected by this issue is the function include of the file /index.php. The manipulation of the argument page results in file	2026-06-03	7.3	CVE-2026-10694

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	inclusion. The attack can be launched remotely. The exploit is now public and may be used.			
SourceCodester--Pizzafy E-Commerce System	A vulnerability was detected in SourceCodester Pizzafy E-Commerce System 1.0. Affected by this vulnerability is the function Login of the file /admin/admin_class_novo.php of the component Administrative Control Panel. The manipulation of the argument Username results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	2026-06-03	7.3	CVE-2026-10704
SourceCodester--SEO Meta Tag Extractor	A vulnerability was determined in SourceCodester SEO Meta Tag Extractor 1.0. This vulnerability affects the function get_headers of the file /index.php. This manipulation of the argument url causes server-side request forgery. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	2026-06-01	7.3	CVE-2026-10287
SourceCodester--Ship Ferry Ticket Reservation System	A security vulnerability has been detected in SourceCodester Ship Ferry Ticket Reservation System up to 1.0. This impacts an unknown function of the file /admin/login.php of the component Admin Login. Such manipulation of the argument Username leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	2026-06-04	7.3	CVE-2026-10877
SourceCodester--Water Billing Management System	A vulnerability has been found in SourceCodester Water Billing Management System 1.0. This issue affects some unknown processing of the file /classes/Users.php?f=save of the component User Management Endpoint. Such manipulation leads to improper authorization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2026-06-01	7.3	CVE-2026-10236
Spacelabs Healthcare--Sentinel	Spacelabs Healthcare Sentinel versions 10.5.x and higher and 11.x.x before 11.6.0 contain an unauthenticated remote code execution vulnerability through a deprecated .NET Remoting HTTP channel exposed on port 8989 that allows attackers to perform arbitrary file read and write operations by supplying valid .NET URI endpoints. Attackers can write ASPX webshells to the IIS wwwroot directory to achieve unauthenticated remote code execution on the system. Port 8989 is not exposed in a default Sentinel installation; exploitation requires that the .NET Remoting port has been explicitly made network-accessible through deliberate configuration or network policy changes.	2026-06-02	9.8	CVE-2026-0611
SQLite--sqldiff	SQLite 'sqldiff.exe' does not securely handle the way the Microsoft Windows C runtime converts Unicode characters to ANSI codepages. An attacker could use the '-L' option to load an arbitrary DLL with a crafted command line argument string that results in command line file arguments being misinterpreted as command line options. Fixed on or around 2025-12-26.	2026-06-04	9.8	CVE-2025-71316
steipete--CodexBar	CodexBar prior to 0.32.0 contains a privilege escalation vulnerability in the CLI installer that allows local attackers to execute arbitrary commands as root by exploiting a race condition in temporary file handling. The installer creates a temporary file with mktemp, writes a privileged shell payload into it, and executes it with administrator privileges via bash, allowing a same-user local process to rewrite the installer body before the administrator prompt is approved, causing attacker-controlled commands to run as root.	2026-06-01	7.1	CVE-2026-49134
steipete--CodexBar	CodexBar prior to 0.32.0 contains an insecure temporary file handling vulnerability that allows local attackers to access sensitive credentials or tamper with build artifacts by exploiting predictable file paths in the release notarization workflow. Attackers with access to the same host can read the App Store Connect API key written to a fixed path, pre-create files or symbolic links at predictable locations to redirect writes to attacker-controlled destinations, or tamper with notarization archives before submission.	2026-06-01	7.1	CVE-2026-49135
SWivid--F5-TTS	F5-TTS through version 1.1.20 contains a path traversal vulnerability in the finetune Gradio handlers that allows unauthenticated attackers to write	2026-06-01	8.2	CVE-2026-43624

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary files by passing unsanitized user-supplied project names directly to <code>os.path.join()</code> without validating the resulting path stays within the intended base directory. Attackers can supply absolute path arguments such as <code>/tmp/EVIL</code> to override the base directory entirely and create arbitrary directories with attacker-controlled JSON content at any filesystem path writable by the server process.			
Synology-- Synology Active Backup for Business Recovery Media Creator	An inclusion of functionality from untrusted control sphere vulnerability in OpenSSL configuration in Synology Active Backup for Business Recovery Media Creator before 2.5.0-2081 allows local users to execute arbitrary code via unspecified vectors.	2026-06-03	7.8	CVE-2022-49036
Synology-- Synology Hyper Backup Explorer	An inclusion of functionality from untrusted control sphere vulnerability in MinGW DLL component in Synology Hyper Backup Explorer before 3.0.1-0156 allows local users to execute arbitrary code via unspecified vectors.	2026-06-03	7.8	CVE-2022-49042
Tautulli--Tautulli	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. Versions prior to 2.17.1 expose a public <code>/image/<hash></code> route that resolves attacker-controlled entries from <code>image_hash_lookup</code> and replays them through the same server-side image fetch logic used by authenticated image proxying. A low-privilege guest user can seed a malicious external image URL into this lookup table and then trigger server-side fetches through a fully unauthenticated endpoint. This turns an authenticated SSRF primitive into a persistent unauthenticated SSRF gadget. Once the malicious hash entry exists, any external user can request <code>/image/<hash>.png</code> and cause the PMS or Tautulli host to fetch an arbitrary attacker-chosen URL. Version 2.17.1 patches the issue.	2026-06-04	9.9	CVE-2026-43986
Tautulli--Tautulli	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. Versions prior to 2.17.1 expose <code>log_js_errors</code> to any authenticated user, including guest users when guest access is enabled. The endpoint writes attacker-controlled strings directly into the main application log. The administrator-only <code>logFile</code> view then reads that log file and embeds it into an HTML response without escaping. This creates a stored cross-site scripting condition where a low-privilege guest can inject HTML or JavaScript into the log file and have it execute in an administrator's browser when the log viewer is opened. Version 2.17.1 patches the issue.	2026-06-04	8.9	CVE-2026-43984
Tautulli--Tautulli	Tautulli is a Python based monitoring and tracking tool for Plex Media Server. Versions prior to 2.17.1 expose <code>configUpdate</code> as a state-changing administrator endpoint, but the route does not enforce <code>POST</code> and does not use any anti-CSRF token. In the default form and JWT-based authentication mode, the administrator session cookie is issued with <code>SameSite=Lax</code> , which still permits top-level cross-site navigation requests. An attacker can exploit this by luring a logged-in administrator to a malicious page that submits a cross-site request to <code>/configUpdate</code> and overwrites the local administrator username and password. The attacker can then sign in directly with the chosen credentials and take over the Tautulli administrative interface. Version 2.17.1 patches the issue.	2026-06-04	8.8	CVE-2026-43985
Termix-SSH-- Termix	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Prior to version 2.3.2, the <code>GET /ssh/file_manager/ssh/resolvePath</code> endpoint in Termix is vulnerable to OS command injection. The endpoint uses double-quote escaping for shell command construction, which does not prevent <code>\$(...)</code> and backtick command substitution. Any authenticated user with an active File Manager SSH session can execute arbitrary commands on the connected remote host. Version 2.3.2 patches the issue.	2026-06-05	9.9	CVE-2026-45744
Termix-SSH-- Termix	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Prior to version 2.3.2, the File Manager functionality in Termix contains a critical Broken Access Control vulnerability due to improper validation of the <code>sessionId</code> parameter. The	2026-06-05	9	CVE-2026-45746

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	backend trusts a client-controlled identifier without verifying that it belongs to the authenticated user. This allows an attacker to manipulate the value and access active File Manager sessions belonging to other users. Since these sessions are tied to SSH connections to remote VPS instances, exploitation allows unauthorized interaction with another user's remote filesystem. Because the File Manager exposes functionality such as file reading, writing, uploading, and execution, this vulnerability enables direct command execution on another user's VPS (RCE). Version 2.3.2 patches the issue.			
Termix-SSH--Termix	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. The `POST /ssh/tunnel/connect` endpoint in Termix prior to version 2.3.2 builds an SSH tunnel command by interpolating user-controlled host record fields (`endpointIP`, `endpointUsername`, `password`) directly into a shell command without escaping, allowing persistent OS command injection on the source SSH host. Version 2.3.2 patches the issue.	2026-06-05	9.8	CVE-2026-45748
Termix-SSH--Termix	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Prior to version 2.3.2, the GET /ssh/file_manager/ssh/resolvePath endpoint in the Termix File Manager component unsafely processes the path parameter and embeds it into a shell command executed over the active SSH session. Because the user-controlled value is placed inside double quotes and only double quotes are escaped, shell command substitution syntax such as \$(...) is still interpreted by the remote shell. Version 2.3.2 fixes the issue.	2026-06-05	9	CVE-2026-45750
Termix-SSH--Termix	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. 16 file-manager endpoints in Termix prior to version 2.3.2 do not verify that the requesting user owns the SSH session identified by `sessionId`. An authenticated attacker who knows or guesses another user's active `sessionId` can read, write, delete, download, and execute files on the victim's connected SSH host. Version 2.3.2 patches the issue.	2026-06-05	8.1	CVE-2026-45743
Termix-SSH--Termix	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. Starting in version 1.7.0, Termix Desktop (Electron) disables TLS certificate validation, allowing a machine-in-the-middle attacker to intercept and modify HTTPS traffic to the configured Termix server. This can lead to credential theft and JWT/session theft during login and normal use. As of time of publication, no known patched versions are available.	2026-06-05	8	CVE-2026-45745
Termix-SSH--Termix	Termix is a web-based server management platform with SSH terminal, tunneling, and file editing capabilities. The `POST /users/totp/disable` and `POST /users/totp/backup-codes` endpoints in Termix prior to version 2.3.2 accept the account password as a sole authentication factor for MFA-critical operations. An attacker who obtains a user's password (phishing, credential stuffing, the passwordHash leak in GHSA-xxxx) can disable TOTP entirely or regenerate backup codes, without ever possessing the TOTP device or knowing a valid TOTP code. This renders two-factor authentication ineffective. Version 2.3.2 patches the issue.	2026-06-05	8.1	CVE-2026-45749
Themefic--Hydra Booking	Missing Authorization vulnerability in Themefic Hydra Booking allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Hydra Booking: from n/a through 1.1.41.	2026-06-01	7.3	CVE-2026-42675
Themeisle--Masteriyo LMS PRO	Incorrect Privilege Assignment vulnerability in Themeisle Masteriyo LMS PRO allows Privilege Escalation. This issue affects Masteriyo LMS PRO: from n/a through 2.20.0.	2026-06-02	9.8	CVE-2025-53209
Themerig--Listing Hub CMS	Listing Hub CMS 1.0 contains a SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send GET requests to pages.php with crafted id values using error-based SQL injection techniques to extract database credentials, usernames, and version information.	2026-06-04	8.2	CVE-2019-25730

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
themeum--Kirki Freeform Page Builder, Website Builder & Customizer	The Kirki - Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions 6.0.0 to 6.0.6. This is due to the plugin accepting an arbitrary email address when a username is used in the password reset request. This makes it possible for unauthenticated attackers to send a password reset link for any user registered on the site to their own email address.	2026-06-02	9.8	CVE-2026-8206
ThimPress--LearnPress	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThimPress LearnPress allows Reflected XSS. This issue affects LearnPress: from n/a through 4.3.6.	2026-06-01	7.1	CVE-2026-48865
ThimPress--Thim Core	Missing Authorization vulnerability leading to code execution after installing malicious vulnerable plugin in ThimPress Thim Core. This issue affects Thim Core: from n/a through 2.3.3.	2026-06-02	8.8	CVE-2025-53345
tittuvarghese--CollegeManagementSystem	A vulnerability was detected in tittuvarghese CollegeManagementSystem 3e476335cfbf9a049e09f474c7ec885f69a9df3/a38852979f7e27ae67b610dce5979500ef8ebe01. This affects an unknown function of the file dashboard_page/forms/fetch.php. Performing a manipulation of the argument department_code results in sql injection. The attack can be initiated remotely. The exploit is now public and may be used. Continuous delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-05	7.3	CVE-2026-11334
Tomdever--wpForo Forum	Missing Authorization vulnerability in Tomdever wpForo Forum allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects wpForo Forum: from n/a through 3.0.6.	2026-06-01	9.1	CVE-2026-42682
UnboundStudio--Accordion FAQ	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UnboundStudio Accordion FAQ allows Reflected XSS. This issue affects Accordion FAQ: from n/a through 2.2.1.	2026-06-02	7.1	CVE-2025-52759
UnboundStudio--Accordion FAQ	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in UnboundStudio Accordion FAQ allows PHP Local File Inclusion. This issue affects Accordion FAQ: from n/a through 2.2.1.	2026-06-02	7.5	CVE-2025-58024
USCiLab--Cereal	A vulnerability was determined in USCiLab Cereal up to 1.3.2. Affected is an unknown function of the component Shared Pointer Handler. Executing a manipulation can lead to type confusion. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure.	2026-06-07	7.3	CVE-2026-11463
UTT--HiPER 1200GW	A vulnerability was detected in UTT HiPER 1200GW up to 2.5.3-170306. This affects the function strcpy of the file /goform/formTaskEdit. The manipulation results in stack-based buffer overflow. The attack may be launched remotely. The exploit is now public and may be used.	2026-06-01	8.8	CVE-2026-10292
UTT--HiPER 1200GW	A flaw has been found in UTT HiPER 1200GW up to 2.5.3-170306. This impacts the function strcpy of the file /goform/formFireWall. This manipulation of the argument Profile causes stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been published and may be used.	2026-06-01	8.8	CVE-2026-10293
VeronaLabs--WP Statistics	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VeronaLabs WP Statistics allows DOM-Based XSS. This issue affects WP Statistics: from n/a through 14.16.6.	2026-06-01	7.1	CVE-2026-48839
vertex-app--vertex	Vertex is a management tool for PT (Private Tracker) users to manage streaming and watching videos. Versions prior to commit fbde301b97986d5913fc4bc95f5445750d282e11 are vulnerable to path traversal. Users should upgrade to a version containing commit fbde301b97986d5913fc4bc95f5445750d282e11 to receive a patch.	2026-06-01	8.6	CVE-2024-40646
Wasiliy Strecker / ContestGallery developer--Contest Gallery Pro	Incorrect Privilege Assignment vulnerability in Wasiliy Strecker / ContestGallery developer Contest Gallery Pro allows Privilege Escalation. This issue affects Contest Gallery Pro: from n/a through 29.0.1.	2026-06-01	9.8	CVE-2026-42680

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
webfactory--Advanced Google reCAPTCHA	The WP Captcha PRO (the premium version of the Advanced Google reCAPTCHA plugin, both have the same slug) plugin for WordPress is vulnerable to arbitrary file upload in all versions up to, and including, 5.38. This is due to a capability check in the save_ajax() function of the licensing module, combined with unrestricted file extraction in sync_cloud_protection(). This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary files including PHP webshells to the server by injecting a malicious cloud_protection_url into the license meta, which the plugin then downloads and extracts without file type validation into a web-accessible uploads directory. This can be used for remote code execution. Note: The vulnerability can only be exploited with a remote URL if "allow_url_fopen" is enabled in the php.ini config.	2026-06-05	8.8	CVE-2026-5411
webfactory--Advanced Google reCAPTCHA	The WP Captcha PRO (the premium version of the Advanced Google reCAPTCHA plugin, both have the same slug) plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 5.38. This is due to the ajax_run_tool() AJAX handler relying solely on a nonce check (check_ajax_referer) for security without performing any capability check, combined with the create_temporary_link tool allowing the generation of passwordless login links for arbitrary users, and the handle_temporary_links() function authenticating visitors via these links without any additional authorization validation. The required nonce is exposed to all authenticated backend users (including Subscribers) via wp_localize_script() on all non-settings admin pages when the plugin's welcome pointer has not been dismissed. This makes it possible for authenticated attackers, with Subscriber-level access and above, to bypass normal authentication and log in as any user, including Administrators, resulting in complete account takeover.	2026-06-05	8.8	CVE-2026-5415
Wp Directory Kit--WP Directory Kit	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Wp Directory Kit WP Directory Kit allows Blind SQL Injection. This issue affects WP Directory Kit: from n/a through 1.5.1.	2026-06-01	9.3	CVE-2026-42672
WP Swings--Wallet System for WooCommerce	Authentication Bypass Using an Alternate Path or Channel vulnerability in WP Swings Wallet System for WooCommerce allows Password Recovery Exploitation. This issue affects Wallet System for WooCommerce: from n/a through 2.7.5.	2026-06-02	7.1	CVE-2026-42654
wpdevteam--Gutenberg Essential Blocks Page Builder for Gutenberg Blocks & Patterns	The Gutenberg Essential Blocks - Page Builder for Gutenberg Blocks & Patterns plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 6.1.3 via the 'save_ai_generated_image()' function. This makes it possible for authenticated attackers, with Author-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	2026-06-04	7.2	CVE-2026-10586
wpusermanager--WP User Manager User Profile Builder & Membership	The WP User Manager - User Profile Builder & Membership plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.9.17 via the (profile template scope) function. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	2026-06-05	7.5	CVE-2026-9290
zauberzeug--nicegui	NiceGUI is a Python-based UI framework. Prior to version 3.12.0, ui.restructured_text() renders reStructuredText server-side with Docutils without disabling file insertion directives. When a NiceGUI application passes attacker-controlled content to ui.restructured_text(), an attacker can use standard Docutils directives (include, csv-table with :file:, raw with :file:) to read local files readable by the NiceGUI server process. Applications that only pass trusted static strings to ui.restructured_text() are not affected. This issue has been patched in version 3.12.0.	2026-06-02	7.5	CVE-2026-45553

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zhayujie--chatgpt-on-wechat	A weakness has been identified in zhayujie chatgpt-on-wechat up to 2.0.8. This issue affects the function _get_safety_warning of the file agent/tools/bash/bash.py of the component Bash Tool. Executing a manipulation can lead to os command injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 2.0.9 is capable of addressing this issue. This patch is called 16d9b449c9aa53ccee44144a762a2737d7ba4fc4. It is recommended to upgrade the affected component.	2026-06-01	7.3	CVE-2026-10214
Zuz--Zuz Music	Zuz Music 2.1 contains a persistent cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious JavaScript by submitting crafted contact form data. Attackers can inject script code through the name, subject, and message parameters in POST requests to /gmusic/zuzconsole/___contact, which executes when administrators view messages in the inbox interface.	2026-06-04	7.2	CVE-2019-25731
AdguardTeam--AdGuardHome	AdGuard Home, when started with the --glinet flag, contains an authentication bypass vulnerability that allows unauthenticated attackers to gain full admin access by supplying a path traversal sequence in the Admin-Token cookie, exploiting unsanitized string concatenation in the token file path construction within the authglinet middleware. Attackers can craft a request with a traversal payload in the Admin-Token header to redirect file reads to arbitrary paths.	2026-06-08	9.4	CVE-2026-41448
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47911
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47912
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47913
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47914
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47915
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47916
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47917
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47918
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47919

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47920
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47921
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an Uncontrolled Search Path Element vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-06-09	7.4	CVE-2026-47937
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47952
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47955
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47959
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-12	7.8	CVE-2026-47965
Adobe--Adobe Campaign Classic (ACC)	Adobe Campaign Classic (ACC) versions 7.4.3 build 9394 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in privilege escalation. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-09	10	CVE-2026-47938
Adobe--Adobe Campaign Classic (ACC)	Adobe Campaign Classic (ACC) versions 7.4.3 build 9394 and earlier are affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-09	10	CVE-2026-48303
Adobe--Adobe Experience Manager Forms JEE	Adobe Experience Manager Forms JEE versions LTS SP1, 6.5.24.0 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field, potentially gaining elevated access or control over the victim's account or session. Scope is changed.	2026-06-09	9.3	CVE-2026-34691
Adobe--Adobe Experience Manager Forms JEE	Adobe Experience Manager Forms JEE versions LTS SP1, 6.5.24.0 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this vulnerability to inject malicious scripts into a web page, potentially gaining elevated access or control over the victim's account or session. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.	2026-06-09	8	CVE-2026-34693
Adobe--CAI Content Credentials	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Integer Overflow or Wraparound vulnerability. An attacker could exploit this vulnerability to crash the application, leading	2026-06-09	7.5	CVE-2026-34711

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to a denial-of-service condition. Exploitation of this issue does not require user interaction.			
Adobe--CAI Content Credentials	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Improper Input Validation vulnerability. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-06-09	7.5	CVE-2026-34712
Adobe--CAI Content Credentials	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Uncontrolled Resource Consumption vulnerability. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-06-09	7.5	CVE-2026-34713
Adobe--ColdFusion	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-09	9.6	CVE-2026-47928
Adobe--ColdFusion	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. A high-privileged attacker could exploit this vulnerability to gain elevated access or control over the victim's account or session. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-09	8.4	CVE-2026-47929
Adobe--ColdFusion	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized read and write access. Exploitation of this issue does not require user interaction.	2026-06-09	8.1	CVE-2026-47930
Adobe--ColdFusion	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-09	8.4	CVE-2026-47931
Adobe--ColdFusion	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to access unauthorized files or directories outside the intended restrictions. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-06-09	8.8	CVE-2026-47932
Adobe--ColdFusion	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-06-09	7.4	CVE-2026-47960
Adobe--Dreamweaver Desktop	Dreamweaver Desktop versions 21.7 and earlier are affected by a Dependency on Vulnerable Third-Party Component vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-06-09	8.6	CVE-2026-47906
Adobe--Dreamweaver Desktop	Dreamweaver Desktop versions 21.7 and earlier are affected by an Improper Access Control vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-06-09	8.2	CVE-2026-47907
Adobe--Dreamweaver Desktop	Dreamweaver Desktop versions 21.7 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-47908

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Format Plugins	Format Plugins versions 1.1.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-48291
Adobe--Format Plugins	Format Plugins versions 1.1.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-48292
Adobe--InCopy	InCopy versions 21.3, 20.5.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-34706
Adobe--InCopy	InCopy versions 21.3, 20.5.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-34707
Adobe--InCopy	InCopy versions 21.3, 20.5.3 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-34708
Adobe--InDesign Desktop	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-34695
Adobe--InDesign Desktop	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-34696
Adobe--InDesign Desktop	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-34697
Adobe--InDesign Desktop	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-34698
Adobe--InDesign Desktop	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-34699
Adobe--InDesign Desktop	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-34700
Adobe--InDesign Desktop	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-34701
Adobe--InDesign Desktop	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-34702
Adobe--InDesign Desktop	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-48293

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--Substance3D - Sampler	Substance3D - Sampler versions 6.0.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-34709
Adobe--Substance3D - Sampler	Substance3D - Sampler versions 6.0.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-34710
Adobe--Substance3D - Sampler	Substance3D - Sampler versions 6.0.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-48305
Adobe--Substance3D - Sampler	Substance3D - Sampler versions 6.0.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8	CVE-2026-48306
Amasty--Order Attributes for Magento 2	Amasty Order Attributes for Magento 2 before version 4.0.0 contains an unauthenticated arbitrary file upload vulnerability that allows unauthenticated attackers to write arbitrary files to the store's media directory by submitting files of any type or name to the upload endpoint without authentication, session validation, or cart context. Attackers can upload PHP files to achieve remote code execution on servers where the media directory permits PHP execution, or alternatively enable malware hosting, stored cross-site scripting via HTML or SVG uploads, and path traversal to write files outside the intended upload directory.	2026-06-12	9.8	CVE-2026-53787
AmentoTech--Doctreat Core	The Doctreat Core plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 1.6.8. This is due to the doctreat_process_registration() function not properly restricting the roles that a user can register with. This makes it possible for unauthenticated attackers to register as an administrator user.	2026-06-10	9.8	CVE-2025-6254
apostrophecms--@apostrophecms/seo	ApostropheCMS is an open-source Node.js content management system. Versions up to and including 1.4.2 of the '@apostrophecms/seo' package injects the Google Analytics Tracking ID ('seoGoogleTrackingId') and Google Tag Manager ID ('seoGoogleTagManager') directly into '<script>' tag bodies using JavaScript template literals without any sanitization or validation. Any user with editor-level access (the default role for content managers) can set these fields to a malicious value, resulting in stored XSS that executes on every page for every visitor of the site. As of time of publication, no known patched versions are available.	2026-06-12	8.7	CVE-2026-53608
apostrophecms--apostrophe	ApostropheCMS is an open-source Node.js content management system. In versions up to and including 4.30.0, 'apos.util.set()' traverses dot-notation paths without sanitizing '__proto__', allowing an authenticated editor to write arbitrary values to 'Object.prototype' via the '\$pullAll' patch operator. A confirmed gadget in 'publicApiCheck()' causes this to bypass authorization on all piece-type REST API endpoints for every subsequent unauthenticated request, for the lifetime of the Node.js process. As of time of publication, no known patched versions are available.	2026-06-12	9.1	CVE-2026-53609
apostrophecms--apostrophe	ApostropheCMS is an open-source Node.js content management system. Versions up to and including 4.29.0 have a password reset flow that constructs the reset URL using 'req.hostname', which is derived directly from the attacker-controlled HTTP 'Host' header when 'apos.baseUrl' is not explicitly configured. An unauthenticated attacker who knows a victim's email address can send a crafted reset request that causes the application to email the victim a reset link pointing to the attacker's domain. When the victim clicks the link, the valid reset token is delivered to the attacker, enabling full account takeover. As of time of publication, no known patched versions are available.	2026-06-12	8.1	CVE-2026-45013

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apostrophecms--apostrophe	ApostropheCMS is an open-source Node.js content management system. Version 4.29.0 has a stored cross-site scripting vulnerability in the image widget functionality. A user with the Editor role can configure an image widget link to use a javascript: URL payload. Because editors have permission to publish pages, the malicious widget can be published to the live site. When another user, including an administrator or public visitor, clicks the affected image/link, arbitrary JavaScript executes in the victim's browser. As of time of publication, no known patched versions are available.	2026-06-12	7.3	CVE-2026-45011
apostrophecms--apostrophe	ApostropheCMS is an open-source Node.js content management system. Versions up to and including 4.29.0 contain an authenticated server-side request forgery (SSRF) in the rich-text widget import flow. An authenticated user who can submit/edit rich-text widget content can cause the server to fetch attacker-controlled URLs during widget validation. For image-compatible responses, the fetched content can be persisted and re-hosted by Apostrophe, allowing response exfiltration. As of time of publication, no known patched versions are available.	2026-06-12	7.6	CVE-2026-45012
apostrophecms--sanitize-html	ApostropheCMS is an open-source Node.js content management system, and sanitize-html provides a simple HTML sanitizer with a clear API. Under the default configuration, versions of `sanitize-html` prior to 2.17.4 can turn attacker-controlled content inside a disallowed `xmp` element into live HTML or JavaScript. This is a sanitizer bypass in the default `disallowedTagsMode: 'discard'` path and can lead to stored XSS in applications that render sanitized output back to users. Version 2.17.4 patches the issue.	2026-06-12	9.3	CVE-2026-44990
Apptha--Apptha Slider Gallery	Apptha Slider Gallery 1.0 contains a path traversal vulnerability that allows unauthenticated attackers to download arbitrary files by manipulating the imgname parameter. Attackers can send requests to asgallDownload.php with directory traversal sequences ../ to access sensitive files outside the intended directory.	2026-06-09	7.5	CVE-2017-20248
apptha--Apptha Slider Gallery	Apptha Slider Gallery 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the albid parameter. Attackers can send GET requests with crafted SQL payloads in the albid parameter to extract sensitive database information including user credentials and authentication hashes.	2026-06-09	8.2	CVE-2017-20249
Apptha--Mac Photo Gallery	Mac Photo Gallery 3.0 contains a path traversal vulnerability that allows unauthenticated attackers to download arbitrary files by manipulating the albid parameter. Attackers can send requests to macdownload.php with directory traversal sequences to access sensitive files like wp-load.php outside the intended plugin directory.	2026-06-09	7.5	CVE-2017-20250
Apptha--PICA Photo Gallery	WordPress Plugin PICA Photo Gallery 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the aid parameter. Attackers can send GET requests with crafted SQL payloads in the aid parameter to extract sensitive database information including user credentials and table contents.	2026-06-09	8.2	CVE-2017-20247
Aqara--Aqara Developer Portal	The Aqara Developer Portal (developer.aqara.com) and shared test environments (developer-test.aqara.com, aiot-test.aqara.com) exhibit cross-origin request sharing, which is an instance of "CWE-942: Permissive Cross-domain Policy with Untrusted Domains," and has an estimated CVSS of CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N (8.2 High).	2026-06-12	8.2	CVE-2026-50088
Aqara--Aqara IAM/SSO Gateway	The Aqara IAM/SSO gateway (gw-builder.aqara.com) exposes bidirectional AES round-trips against the platform's signing key without authentication. This is an instance of "CWE-306: Missing Authentication for Critical Function" and "CWE-327: Use of a Broken or Risky Cryptographic Algorithm," and has an estimated CVSS of CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N (7.5 High).	2026-06-12	10	CVE-2026-50086

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Aqara--Aqara IAM/SSO Gateway	The Aqara IAM/SSO gateway (gw-builder.aqara.com) exhibits a cross-origin request sharing vulnerability, which is an instance of "CWE-942: Permissive Cross-domain Policy with Untrusted Domains," and has an estimated CVSS of CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N (8.2 High).	2026-06-12	8.2	CVE-2026-50087
Aqara--Aquara IAM/SSO Gateway	The Aqara IAM/SSO Gateway (gw-builder.aqara.com) used a hardcoded OAuth client credential, which is an instance of "CWE-798: Use of Hard-coded Credentials." This issue has an estimated CVSS of CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N (9.1 Critical). When combined with CVE-2026-50082, CVE-50084, and CVE-50085, this can lead to a fully unauthenticated, remote takeover of affected devices.	2026-06-12	9.1	CVE-2026-50083
Aqara--Board service	The Aqara Board service (op-test.aqara.com) accepts arbitrary MQTT command payloads, and forwards them to the platform's HiveMQ broker without authentication. This is an instance of "CWE-306: Missing Authentication for Critical Function" and has an estimated CVSS of CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L (8.6 High). When combined with CVE-2026-50082, CVE-50083, and CVE-50084, this can lead to a fully unauthenticated, remote takeover of affected devices.	2026-06-12	8.6	CVE-2026-50085
Aqara--Cloud OAuth Authorization Endpoint	The Aqara Cloud OAuth Authorization Endpoint (open-cn.aqara.com/oauth/authorize) is vulnerable to a redirect bypass due to lax controls on domain matching, which is an instance of "CWE-1289: Improper Validation of Unsafe Equivalence in Input" and has an estimated CVSS of CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N (9.3 Critical).	2026-06-12	9.3	CVE-2026-50090
Aqara--Cloud Production API	The Aqara Cloud Production API (open-cn.aqara.com/v3.0/open/api) would authorize any valid developer token for access to any account. This is an instance of "CWE-862: Missing Authorization" with an estimated CVSS of CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N (9.6 Critical). When combined with CVE-2026-50082, CVE-50083, and CVE-50085, this can lead to a fully unauthenticated, remote takeover of affected devices.	2026-06-12	9.6	CVE-2026-50084
Aqara--com.lumiunited.aqarahome	Aqara Home Android (com.lumiunited.aqarahome) 6.0.0 (and white-label clients embedding the same liblumidevsdk.so) uses hard-coded cryptographic keys, which is an instance of "CWE-321: Use of Hard-coded Cryptographic Key" and has an estimated CVSS of CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N (9.1 Critical).	2026-06-12	9.1	CVE-2026-50091
ArnasDon--wacrm	WACRM prior to commit 73041bf contain an authorization bypass vulnerability in the automation engine that allows authenticated attackers to access and modify contacts belonging to other tenants by supplying an arbitrary caller-controlled contact_id in the POST request body without tenant ownership verification. Attackers can exploit the service-role client that bypasses row-level security to modify victim contact fields including name, email, and company across tenant boundaries using only a known contact UUID.	2026-06-08	7.1	CVE-2026-49141
AWS--AgentCore CLI	Improper neutralization of triple-quote characters during Python code generation in AgentCore CLI before v0.14.2 might allow an authenticated remote threat actor to execute arbitrary code on AWS AgentCore Runtime under the imported agent's IAM execution role and on the local environment of another user in the same AWS account, via a crafted collaborationInstruction stored on a Bedrock Agent collaborator and later processed by that other user during agent import. To remediate this issue, users should upgrade to version 0.14.2.	2026-06-08	9	CVE-2026-11393
AWS--AWS Cloud Development Kit library	OS command injection in the NodejsFunction local bundling pipeline in aws-cdk-lib before 2.245.0 (2.246.0 on Windows) might allow an actor who controls the value of one or more bundling properties (externalModules, define, loader, inject, or esbuildArgs) to execute arbitrary commands on the host running the CDK toolchain via injected shell metacharacters. This issue requires the threat actor to control the value of one or more of the affected bundling properties in the CDK application. To remediate this issue, users should upgrade to aws-cdk-lib 2.245.0 (2.246.0 on Windows) or later.	2026-06-10	7.3	CVE-2026-11417

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
AWS--aws-c-http	Improper handling of HPACK dynamic table size updates in the AWS Common Runtime aws-c-http library might allow a remote threat actor operating a server to cause memory corruption on a connecting client application, potentially leading to arbitrary code execution, via a crafted sequence of HTTP/2 HEADERS frames. To remediate this issue, users should upgrade to aws-c-http version 0.11.0.	2026-06-12	8.8	CVE-2026-12043
axios--axios	Axios is a promise based HTTP client for the browser and Node.js. Prior to 0.32.0 and 1.16.0, Axios does not normalise IPv4-mapped IPv6 addresses. When NO_PROXY lists an IPv4 address such as 127.0.0.1 or 169.254.169.254, a request URL using the IPv4-mapped IPv6 form (::ffff:7f00:1, ::ffff:a9fe:a9fe) still routes through the configured proxy. Node.js resolves these addresses to the underlying IPv4 host, so the request reaches the internal service via the proxy rather than being blocked. This vulnerability is fixed in 0.32.0 and 1.16.0.	2026-06-11	8.6	CVE-2026-44492
axios--axios	Axios is a promise based HTTP client for the browser and Node.js. From 1.0.0 to before 1.16.0, the Axios library is vulnerable to a Prototype Pollution "Gadget" attack that allows any Object.prototype pollution in the application's dependency tree to be escalated into a full Man-in-the-Middle (MITM) attack - intercepting, reading, and modifying all HTTP traffic including authentication credentials. The HTTP adapter at lib/adapters/http.js:670 reads config.proxy via standard property access, which traverses the prototype chain. Because proxy is not present in Axios defaults, the merged config object has no own proxy property, making it trivially injectable via prototype pollution. Once injected, setProxy() routes all HTTP requests through the attacker's proxy server. This vulnerability is fixed in 1.16.0.	2026-06-11	8.7	CVE-2026-44494
axios--axios	Axios is a promise based HTTP client for the browser and Node.js. Prior to 0.32.0 and 1.16.0, Axios' Node.js HTTP adapter can leak proxy credentials to a redirect target in affected versions. When a request is sent through an authenticated proxy, Axios may add a Proxy-Authorization header. If Axios then follows a redirect and the redirected request is no longer sent through that proxy, the stale Proxy-Authorization header can remain on the redirected request and be sent to the redirect target. This affects Node.js's use of Axios with automatic redirects enabled and an authenticated proxy configuration. Browser adapters are not affected. This vulnerability is fixed in 0.32.0 and 1.16.0.	2026-06-11	7.5	CVE-2026-44486
axios--axios	Axios is a promise based HTTP client for the browser and Node.js. Axios versions 1.7.0 through 1.15.x did not enforce configured request and response size limits when requests were sent with the fetch adapter. Applications that selected adapter: 'fetch', or ran in environments where axios resolved to the fetch adapter, could receive or send bodies larger than maxContentLength or maxBodyLength despite those limits being explicitly configured. This can cause resource exhaustion in server-side usage when a malicious or compromised server returns an oversized response, when an attacker can supply a large data: URL, or when an application forwards attacker-controlled request bodies through axios while relying on maxBodyLength as a boundary. This vulnerability is fixed in 0.32.0 and 1.16.0.	2026-06-11	7.5	CVE-2026-44488
axios--axios	Axios is a promise based HTTP client for the browser and Node.js. From 0.19.0 to before 0.31.1 and 1.15.2, Axios contains prototype-pollution gadgets in request config processing. If another vulnerability in the same JavaScript process has already polluted Object.prototype.transformResponse, affected Axios versions may treat that inherited value as request configuration or as an option validator. Axios does not itself create the prototype pollution. Exploitability requires a separate prototype-pollution vulnerability or equivalent attacker control over Object.prototype before Axios creates a request. This vulnerability is fixed in 0.31.1 and 1.15.2.	2026-06-11	7	CVE-2026-44495

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
axios--axios	Axios is a promise based HTTP client for the browser and Node.js. Axios versions before 0.32.0 on the 0.x line and before 1.16.0 on the 1.x line build a regular expression from the configured XSRF cookie name without escaping regex metacharacters. In standard browser environments, an attacker who can influence the cookie name passed to axios can cause expensive regex backtracking while axios reads document.cookie. The practical impact is client-side availability degradation, such as freezing the affected browser tab while axios prepares a request. The issue does not affect ordinary Node.js HTTP adapter usage, React Native, or web workers, where axios does not read document.cookie. This vulnerability is fixed in 0.32.0 and 1.16.0.	2026-06-11	7.5	CVE-2026-44496
Baarsoft Information Technologies Inc.--Rotaban	Unrestricted upload of file with dangerous type vulnerability in BaÅŸarsoft Information Technologies Inc. Rotaban allows Upload a Web Shell to a Web Server. This issue affects Rotaban: from V2026.06.002 before V2026.06.003.	2026-06-11	9.9	CVE-2026-11839
Babelen Group Food Cafe Businesses Industry and Trade Ltd. Co.--Pause+ Mobile App	Improper restriction of excessive authentication attempts vulnerability in BaÅŸbelen Group Food Cafe Businesses Industry and Trade Ltd. Co. Pause+ Mobile App allows Authentication Bypass. This issue affects Pause+ Mobile App: from v1.0.6 before v1.5.	2026-06-12	9.8	CVE-2026-6853
background-image-cropper--Background Image Cropper	WordPress Background Image Cropper version 1.2 contains a remote code execution vulnerability that allows unauthenticated attackers to upload arbitrary files by accessing the ups.php endpoint. Attackers can upload PHP files through the file upload form in the plugin directory to execute arbitrary code on the server.	2026-06-08	9.8	CVE-2024-58348
Beardev--JoomSport	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Beardev JoomSport allows Blind SQL Injection. This issue affects JoomSport: from n/a through 5.7.7.	2026-06-11	9.3	CVE-2026-42647
bludit--bludit	Bludit is a content management system. Versions prior to 3.22.0 have a Broken Access Control flaw where active sessions remain valid even after the corresponding user account has been physically deleted from the database. This "Ghost Session" allows revoked users to maintain full unauthorized access to the system. Version 3.22.0 fixes the issue.	2026-06-08	8.8	CVE-2026-46656
bludit--bludit	Bludit is a content management system. Versions prior to 3.22.0 have a vulnerability in the user management logic that allows deactivated accounts to maintain access via persistent authentication tokens. When an administrator disables a user account, the application fails to invalidate or clear the associated tokenAuth and tokenRemember fields in the JSON database. Consequently, any user with a pre-existing "Remember Me" cookie can bypass the account disablement and maintain a valid authenticated state. Version 3.22.0 patches the issue.	2026-06-08	7.1	CVE-2026-46657
boxlite-ai--boxlite	Boxlite is a sandbox service that allows users to create lightweight virtual machines (Boxes) and launch OCI containers within them to run untrusted code. Prior to version 0.9.0, Boxlite does not restrict the kernel capabilities available inside the container, malicious code can remount the directory in rw mode, thereby gaining write access to that directory. This allows malicious code to perform arbitrary write operations on directories that should be read-only. This issue has been patched in version 0.9.0.	2026-06-10	10	CVE-2026-46695
boxlite-ai--boxlite	Boxlite is a sandbox service that allows users to create lightweight virtual machines (Boxes) and launch OCI containers within them to run untrusted code. Prior to version 0.9.0, Boxlite allows users to specify the OCI image used by containers in the sandbox. However, when processing tar entries in OCI images, Boxlite does not account for the possibility that entries may be symlinks pointing to absolute paths. An attacker can craft a malicious OCI image and distribute it on image hosting platforms such as DockerHub, tricking users into using it. Once a user loads the malicious image, the attacker can write arbitrary content to any path on the host, which can	2026-06-10	9.6	CVE-2026-46703

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	further lead to remote code execution on the host. This issue has been patched in version 0.9.0.			
Brickcom--Cube	Brickcom cameras ship with default credentials that allows any unauthenticated remote attacker to silently access camera feeds.	2026-06-11	7.7	CVE-2026-50005
Brickcom--Cube	Brickcom cameras allow unauthenticated access to live snapshot images via the /ONVIF endpoint and no authentication is required to retrieve still images from the camera feed.	2026-06-11	7.7	CVE-2026-50245
BuddyPress--BuddyPress	BuddyPress 14.4.0 contains an insecure direct object reference vulnerability in the messages REST API that allows authenticated attackers to access arbitrary private message threads by supplying a user_id parameter in the request. Attackers can pass another user's identifier to the get_item_permissions_check method, which validates the supplied user_id instead of the logged-in user and is reused by the update and delete handlers, to read, reply to, or delete any user's private messages.	2026-06-09	8.1	CVE-2026-53673
BuddyPress--BuddyPress	BuddyPress 14.4.0 contains a regular expression injection vulnerability in the activity mention resolver that, when username compatibility mode is enabled, allows attackers to manipulate a REGEXP database clause by crafting mention names containing regex metacharacters. Attackers can submit @mentions whose metacharacters pass through esc_sql unescaped and are inserted into an unprepared REGEXP query against the users table, enabling boolean-based inference of usernames and denial of service through catastrophic backtracking.	2026-06-09	7.1	CVE-2026-53674
Cap-go--Cap-go	Cap-go prior to 12.128.2 contains an account takeover vulnerability in its email change mechanism that allows an attacker with temporary authenticated session access to change the registered email address without re-authentication such as password or MFA verification. Attackers can redirect verification to an attacker-controlled email address and subsequently perform a password reset to permanently take over the victim's account.	2026-06-12	7.6	CVE-2026-53981
Capgo--Capgo	Capgo before 12.128.2 contains a denial of service vulnerability allowing attackers to register accounts using arbitrary email addresses without verification, then initiate deletion to lock emails in pending deletion state. Attackers can permanently lock legitimate users out of the platform for 30 days by exploiting unverified email ownership in account lifecycle operations.	2026-06-12	7.5	CVE-2026-53868
Cellopoint--CelloOS	The SSH service of CelloOS developed by Cellopoint has an Improper Access Control vulnerability, allowing authenticated remote attackers to bypass the enforced command restrictions and execute operating system commands outside the originally authorized scope.	2026-06-12	8.8	CVE-2026-12059
checkpoint--Identity Agent	A local privilege escalation vulnerability exists in Check Point Identity Agent Full for Windows OS. An authenticated local user may be able to execute arbitrary code with SYSTEM privileges due to improper handling of executable resolution during the log collection process. Successful exploitation could allow an attacker to gain elevated privileges on the affected Windows endpoint.	2026-06-11	7.8	CVE-2026-10847
checkpoint--Quantum Security Gateway	A weakness in the certificate validation logic of the deprecated IKEv1 key exchange may allow an unauthenticated attacker positioned as a man-in-the-middle to bypass certificate validation in VPN site-to-site connections that use certificate-based authentication. Successful exploitation could allow interception or modification of traffic traversing the VPN tunnel.	2026-06-08	7.4	CVE-2026-50752
Cloud Foundry--UAA	Cloud Foundry UAA incorrectly treated XML encryption to the Service Provider (confidentiality) as a substitute for XML signatures from the Identity Provider (authenticity) in two SAML flows: the OAuth 2.0 SAML2 bearer grant (token endpoint) and browser SSO (ACS) when wantAssertionSigned is set to false. Assertions or responses that were unsigned but contained encrypted content could still be accepted. Encryption uses the SP's public key from published metadata, therefore, any party, not only a trusted IdP, can produce ciphertext UAA can decrypt; successful decryption therefore does not prove the IdP issued the	2026-06-11	9	CVE-2026-41005

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	message. Affected versions: Cloud Foundry UAA (uaa_release) 2.0.0 through 78.13.0. Cloud Foundry CF Deployment all versions through 56.1.0.			
code-projects--Online Music Site	A vulnerability was found in code-projects Online Music Site 1.0. This vulnerability affects unknown code of the file /Administrator/PHP/AdminDeleteAlbum.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	2026-06-08	7.3	CVE-2026-11489
code-projects--Online Music Site	A vulnerability was determined in code-projects Online Music Site 1.0. This issue affects some unknown processing of the file /Frontend/Search.php. This manipulation of the argument Category causes sql injection. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized.	2026-06-08	7.3	CVE-2026-11490
code-projects--Simple Flight Ticket Booking System	A vulnerability has been found in code-projects Simple Flight Ticket Booking System 1.0. This affects an unknown part of the file checkUser.php of the component POST Parameter Handler. The manipulation of the argument Username leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	2026-06-08	7.3	CVE-2026-11488
code16--sharp	Sharp is a content management framework built for Laravel as a package. Prior to version 9.22.0, Sharp exposes a generic download endpoint that authorizes access only to the supplied Sharp entity instance, but then reads the target storage disk and path from request parameters. Because the requested storage object is not bound to the authorized entity instance, an authenticated Sharp user who can view one valid record may use that record as an authorization anchor to download unrelated disk-relative objects from configured Laravel Storage disks. The confirmed impact is authenticated disclosure of unrelated objects from configured Laravel Storage disks. This issue does not imply arbitrary host filesystem access outside configured Laravel Storage disk roots. This issue has been patched in version 9.22.0.	2026-06-10	7.7	CVE-2026-44692
CodeAstro--Student Attendance Management System	A flaw has been found in CodeAstro Student Attendance Management System 1.0. The impacted element is an unknown function of the file /attendance-php/index.php. Executing a manipulation of the argument Username can lead to sql injection. The attack may be performed from remote. The exploit has been published and may be used.	2026-06-08	7.3	CVE-2026-11582
Comma AI--Openpilot	A vulnerability was found in Comma AI Openpilot 0.11. This issue affects the function pickle.load/pickle.loads of the file selfdrive/modeld/modeld.py of the component Pickle Module. The manipulation results in deserialization. The attack is only possible with local access. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-14	7.8	CVE-2026-12191
commenthol--md-fileserver	md-fileserver allows for local viewing of markdown files in a browser. Prior to version 1.10.3, a cross-site scripting (XSS) vulnerability exists in the application's Markdown rendering logic. When user-supplied Markdown content is rendered, embedded raw HTML-including <script> tags-is processed and injected into the resulting page without sanitization, allowing arbitrary JavaScript execution in the context of the affected domain. This issue has been patched in version 1.10.3.	2026-06-09	7.2	CVE-2026-46492
contrid--Newsletters	The Newsletters plugin for WordPress is vulnerable to time-based SQL Injection via the 'wpmlsubscriber_id' parameter in all versions up to, and including, 4.13 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-06-10	7.5	CVE-2026-3018
creativethemeshq--Blocksy	The Blocksy theme for WordPress is vulnerable to PHP Object Injection leading to Remote Code Execution via the 'blocksy_meta' REST API field and the V200 database migration in versions up to and including 2.1.35.	2026-06-09	8.8	CVE-2026-8365

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This is due to insufficient input sanitization in the <code>blocksy_sanitize_post_meta_options()</code> function, which only blocks values containing '<' or '>' and does not prevent serialized PHP object strings from being stored in post meta, combined with the <code>SearchReplacer::run_recursively()</code> function unconditionally deserializing all string values via <code>@unserialize()</code> during migration without restricting allowed classes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject a serialized <code>Blocksy\RaiiPattern</code> object into post meta that, when the V200 migration runs on an upgraded site, is deserialized and triggers <code>RaiiPattern::__destruct()</code> , which executes arbitrary PHP callables via <code>call_user_func()</code> .			
D-Link--DCS-935L	A security vulnerability has been detected in D-Link DCS-935L 1.10.01. This issue affects the function <code>sprintf</code> of the file <code>/web/cgi-bin/greece/rhea</code> of the component HTTP Handler. Such manipulation of the argument data leads to format string. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	2026-06-13	8.8	CVE-2026-12174
Dana Powers--kafka-python	kafka-python prior to 2.3.2 contains a denial-of-service vulnerability in the protocol parser that allows a malicious broker or machine-in-the-middle attacker to exhaust memory or hang connections by sending a crafted 4-byte frame length value without bounds validation. Attackers can send a specially crafted frame length through the <code>receive_bytes()</code> function to trigger either a multi-gigabyte memory allocation or an uncaught <code>ValueError</code> that leaves the connection in a broken state, causing requests to hang and consumers to stop heartbeating until restart.	2026-06-10	7.5	CVE-2026-10142
Dana Powers--kafka-python	kafka-python prior to 2.3.2 contains a denial-of-service vulnerability in SCRAM authentication handling that allows a malicious or machine-in-the-middle broker to freeze the client event loop by supplying an excessively large iteration count. In <code>scram.py</code> , <code>ScramClient.process_server_first_message()</code> passes the broker-controlled SCRAM iteration count directly to <code>hashlib.pbkdf2_hmac()</code> without validation, blocking producer sends, consumer polls, admin operations, and heartbeats, which can cause consumer group eviction and repeated reconnect failures.	2026-06-10	7.5	CVE-2026-10143
davidanderson--UpdraftPlus: WP Backup & Migration Plugin	The UpdraftPlus: WP Backup & Migration Plugin plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.26.4 via the <code>UpdraftPlus_Remote_Communications_V2::wp_loaded</code> function. This is due to insufficient validation of the remote communications message format, where signature verification can be bypassed and unchecked decryption return values collapse to a predictable all-zero encryption key. This makes it possible for unauthenticated attackers to forge arbitrary RPC commands and run them as the connected administrator, such as uploading and activating a malicious plugin, which ultimately leads to remote code execution.	2026-06-11	8.1	CVE-2026-10795
debev--nanoMODBUS	nanoMODBUS through v1.23.0 contains an off-by-one buffer overflow in the <code>recv_msg_header()</code> function of the Modbus/TCP server that allows remote unauthenticated attackers to write one attacker-controlled byte past the end of the 260-byte receive buffer by sending a crafted MBAP frame whose Length field is set to 255. The overflow corrupts the adjacent buffer-index field of the nanoMODBUS state structure, resulting in denial of service through invalid memory accesses and, on bare-metal and RTOS targets without memory protection, one-byte information disclosure and writes to unintended register addresses on the Write Multiple Registers (FC16) handler path.	2026-06-14	8.6	CVE-2026-54410
degit--degit	Versions of the package degit before 2.8.6, from 3.0.0 and before 3.3.1 are vulnerable to Command Injection due to improper sanitisation of user input for git shell commands directly invoked with <code>exec()</code> method by <code>_cloneWithGit()</code> and <code>fetchRefs()</code> functions. An attacker can execute	2026-06-09	8.8	CVE-2026-11572

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary operating system commands as the process user by supplying a specially crafted git repository name.			
discourse--discourse	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.4, 2026.3.0-latest to before 2026.3.1, and 2026.4.0-latest to before 2026.4.1, chat events for public category channels are published to MessageBus without permission scoping, so any MessageBus subscriber without chat enabled could receive chat message payloads in real time. This issue has been patched in versions 2026.1.4, 2026.3.1, 2026.4.1, and 2026.5.0-latest.1.	2026-06-12	7.5	CVE-2026-44786
driftregion--iso14229	driftregion iso14229 through 0.9.0 contains an integer underflow and downstream out-of-bounds read in the Handle_0x27_SecurityAccess() function in iso14229.c that allows a remote unauthenticated attacker to crash a UDS server and potentially read memory past the receive buffer by sending a single-byte 0x27 SecurityAccess request that follows any earlier well-formed 0x27 message. The handler reads the SecurityAccess subFunction from recv_buf[1] without first checking that recv_len is at least 2, then computes the key-data length as the unsigned subtraction (uint16_t)(recv_len - UDS_0X27_REQ_BASE_LEN); when recv_len equals 1 the result underflows to 65535 and is passed as args.len to the application's SecAccessValidateKey or SecAccessRequestSeed callback, which typically iterates or copies that many bytes from the 4-KB receive buffer. Every other UDS sub-function handler in the library (0x10, 0x11, 0x14, 0x19, 0x22, 0x23, 0x28, and others) performs an explicit recv_len lower-bound check before indexing; Handle_0x27_SecurityAccess is the sole outlier. The vulnerable handler reaches over CAN bus, OBD-II, ISO-TP, and DoIP transports and is exposed in the default diagnostic session without prior authentication; deployments on automotive ECUs, industrial controllers, and IoT devices that ship iso14229 as their UDS server are affected.	2026-06-14	8.2	CVE-2026-54413
DTStack--Taier	A vulnerability was determined in DTStack Taier up to 1.4.0. The affected element is the function preHandle of the file taier-data-develop/src/main/java/com/dtstack/taier/develop/interceptor/LoginInterceptor.java of the component Source Connection Test Endpoint. Executing a manipulation can lead to improper authentication. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. This patch is called f95389e7f74acec42bcee079a616aaa06f9551d2. A patch should be applied to remediate this issue.	2026-06-09	7.3	CVE-2026-11618
emarket-design--Customer Support Ticket System & Helpdesk	The WP Ticket plugin for WordPress is vulnerable to SQL Injection via the WordPress search query parameter (`s`) in versions up to, and including, 6.0.4 The plugin hooks WordPress's `posts_request` filter with `wp_ticket_com_posts_request()`, which calls `emd_author_search_results()` when the current request is an unauthenticated front-end search. That function reads `\$query->query_vars['s']` - already wp_unslash()'d by `WP_Query::parse_query()`, so wp_magic_quotes protection has been stripped - and concatenates the raw value into a SQL `LIKE` clause inside a UNION sub-SELECT appended to the main query, with no `\$wpdb->prepare()` or escaping. This makes it possible for unauthenticated attackers to append additional SQL queries into already-existing queries that can be used to extract sensitive information from the database.	2026-06-13	7.5	CVE-2026-9848
espressif--esp-idf	ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. In versions 5.5.4 and 6.0, the esp_tee component exposes secure-service wrappers in esp_secure_services.c and esp_secure_services_iram.c that bridge calls from the user application (i.e. the REE) to TEE-protected hardware peripherals (AES, SHA, ECC, HMAC, SPI, MMU, WDT) and to the security feature like attestation, OTA updates, secure storage. This issue has been patched in versions 5.5.5 and 6.0.1.	2026-06-10	9.3	CVE-2026-45328

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
espressif--esp-idf	ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. In versions 5.5.4 and 6.0, several ESP-TEE secure-service wrappers in esp_secure_services.c and esp_secure_services_iram.c validated only some of the caller-supplied pointer arguments, leaving input pointer arguments unchecked. Because the underlying TEE-protected hardware peripherals (e.g., ECC, SHA, SPI) run in RISC-V machine mode (M-mode) with full address-space access, a caller could supply pointers into TEE-exclusive memory as inputs, causing the peripheral to read TEE memory and return results derived from it to the REE. Depending on the wrapper, the result contains raw bytes from TEE memory, a computed function of TEE memory recoverable through repeated calls, or a single bit per call that forms an oracle for incremental disclosure of TEE-resident sensitive data. This issue has been patched in versions 5.5.5 and 6.0.1.	2026-06-10	7.1	CVE-2026-45329
espressif--esp-idf	ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. In versions 5.2.6, 5.3.5, 5.4.4, 5.5.4, and 6.0, a NULL-pointer dereference exists in the WebSocket subprotocol-negotiation path of the esp_http_server component. While parsing the client-supplied Sec-WebSocket-Protocol request header during the WebSocket handshake, the tokenisation result is dereferenced without a NULL check, so a malformed header value can crash the server before any application-level authentication runs. This issue has been patched in versions 5.2.7, 5.3.6, 5.4.5, 5.5.5, and 6.0.1.	2026-06-10	7.5	CVE-2026-45541
espressif--esp-idf	ESF-IDF is the Espressif Internet of Things (IOT) Development Framework. In versions 5.2.6, 5.3.5, 5.4.4, 5.5.4, and 6.0, a heap buffer overflow exists in the Security Scheme 2 (SRP6a) session-setup path of the protocomm component. The first-phase handler (handle_session_command0()) in components/protocomm/src/security/security2.c trusts the length of a client-supplied protobuf field for the SRP6a username and copies it into a buffer whose size is derived from a narrower destination type. The resulting truncation-versus-copy asymmetry corrupts the heap when an oversized value is supplied. This issue has been patched in versions 5.2.7, 5.3.6, 5.4.5, 5.5.5, and 6.0.1.	2026-06-10	7.1	CVE-2026-45542
Eugeniy--russh	Russh is a Rust SSH client & server library. Prior to version 0.60.3, CryptoVec used unchecked capacity growth, unchecked length arithmetic, and unsafe allocation/locking paths. In current russh releases, local SSH agent peers could still feed attacker-controlled frame lengths into buffer growth before validation. In older russh releases before 0.58.0, remote SSH traffic also reached CryptoVec through transport and compression buffers. This issue has been patched in version 0.60.3.	2026-06-10	7.5	CVE-2026-46673
Eugeniy--russh	Russh is a Rust SSH client & server library. From version 0.34.0 to before version 0.61.1, when SSH compression is enabled, russh accepted compressed packets whose on-wire size passed the normal transport packet-length checks but whose decompressed size was much larger. This allowed a remote peer to send oversized post-decompression packets that should have been rejected. In current releases, this is a remote denial-of-service / resource-exhaustion issue in the post-decompression receive path. In older releases before 0.58.0, the same remote decompression path used CryptoVec, which appears to make the historical impact worse. This issue has been patched in version 0.61.1.	2026-06-10	7.5	CVE-2026-46702
Eugeniy--russh	Russh is a Rust SSH client & server library. From version 0.34.0 to before version 0.61.0, several russh client and server message handlers decoded attacker-controlled SSH strings, name-lists, and byte fields into owned allocations before applying field-specific bounds. A remote SSH peer could send oversized, high-fanout, or malformed length-prefixed fields and make the library allocate, attempt to allocate, or split data before rejecting input that should have been rejected earlier. This issue has been patched in version 0.61.0.	2026-06-10	7.5	CVE-2026-48110
EvWill--Product Catalog 8	Product Catalog 8 1.2 plugin for WordPress contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary	2026-06-09	8.2	CVE-2016-20065

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	SQL queries by injecting malicious code through the selectedCategory parameter. Attackers can submit POST requests to the admin-ajax.php endpoint with the UpdateCategoryList action to extract sensitive database information from WordPress tables.			
fedify-dev--fedify	Fedify is a TypeScript library for building federated server apps powered by ActivityPub. Fedify previously addressed SSRF/internal network access in GHSA-p9cg-vqcc-grcx by adding public URL validation before runtime document and media fetching. However, the IPv4 validation logic present starting in version 0.11.2 and prior to versions 1.9.12, 1.10.11, 2.0.19, 2.1.15, and 2.2.4 appears incomplete. The `validatePublicUri()` protection relies on `isValidPublicIPv4Address()` to reject non-public IPv4 destinations. The function blocks common private and local ranges such as `10.0.0.0/8`, `127.0.0.0/8`, `169.254.0.0/16`, `172.16.0.0/12`, and `192.168.0.0/16`, but it still treats several special-use, reserved, multicast, benchmarking, and carrier-grade NAT IPv4 ranges as valid public destinations. Because this validation is used as an SSRF defense before outbound fetches, this appears to be an incomplete mitigation or bypass class for the previous SSRF issue. Versions 1.9.12, 1.10.11, 2.0.19, 2.1.15, and 2.2.4 contain an updated patch.	2026-06-10	8.6	CVE-2026-50131
fedify-dev--fedify	Fedify is a TypeScript library for building federated server apps powered by ActivityPub. Prior to versions 1.9.11, 1.10.10, 2.0.18, 2.1.14, and 2.2.3, an attacker can make use of JSON-LD features to restructure a JSON-LD document that would change how Fedify interprets it without changing its Linked Data Signature, allowing them to alter a third-party signed activity they have received. Versions 1.9.11, 1.10.10, 2.0.18, 2.1.14, and 2.2.3 fix the issue.	2026-06-10	7	CVE-2026-42462
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.23.0, the Fission router registers an internal-style route - /fission-function/<name> and /fission-function/<ns>/<name> - for every Function object, independent of whether any HTTPTrigger exists for that function. The route was mounted on the same listener as user-defined HTTPTriggers (svc/router, port 8888), so any caller who could reach the router could invoke any function by guessing its metadata.name (and namespace), bypassing the host / path / method / method-allow-list restrictions encoded in HTTPTrigger objects. This issue has been patched in version 1.23.0.	2026-06-10	9.8	CVE-2026-46614
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.24.0, the Environment.spec.runtime.podSpec / spec.builder.podSpec passthrough lacked validation, and MergePodSpec propagated dangerous fields into the generated pods. This issue has been patched in version 1.24.0.	2026-06-10	9.9	CVE-2026-50545
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.24.0, Fission's Container Executor path lets a tenant supply Function.spec.podspec directly; the executor merges it into the executor-built podspec and creates a Deployment whose pods run the user's container image. This issue has been patched in version 1.24.0.	2026-06-10	9.9	CVE-2026-50563
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.24.0, Fission's Environment CRD exposes spec.runtime.podSpec and spec.builder.podSpec, which are merged into the Kubernetes pod specs for runtime and builder pods. The merge logic propagated hostNetwork, hostPID, hostIPC, container privileged, and serviceAccountName from the user-supplied podspec with no filtering, and Environment.Validate performed no security-relevant checks on these fields. This issue has been patched in version 1.24.0.	2026-06-10	9.9	CVE-2026-50564

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.24.0, a tenant with environments.fission.io create/update RBAC can run privileged / allowPrivilegeEscalation / dangerous-capability containers in the Fission function or builder namespace, scheduled under the executor's high-privilege service account - enabling container-sandbox escape, host filesystem and network access, and potential node- and cluster-level compromise. This issue has been patched in version 1.24.0.	2026-06-10	9.9	CVE-2026-50566
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.23.0, the Fission storagesvc component registers archive CRUD handlers (/v1/archive GET / POST / DELETE and /v1/archives list) directly on its HTTP router without performing any authentication or authorization. Any caller able to reach the storagesvc ClusterIP - including any other workload in the same Kubernetes cluster - could enumerate archive IDs, download archives belonging to other tenants, upload arbitrary archive content, and delete archives. This issue has been patched in version 1.23.0.	2026-06-10	8.8	CVE-2026-46612
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.24.0, the Fission Function admission webhook (pkg/webhook/function.go) validated that spec.secrets[].namespace and spec.configmaps[].namespace equalled the function's own namespace but performed no equivalent check on spec.environment.namespace. This issue has been patched in version 1.24.0.	2026-06-10	8.5	CVE-2026-49824
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.25.0, Fission added PodSpec safety validation for tenant-facing Environment and Function CRDs (ValidatePodSpecSafety / ValidateContainerSafety admission webhook + sanitizeContainerSecurityContext executor merge layer), but the capability check was implemented as a fixed denylist of six Linux capabilities (SYS_ADMIN, NET_ADMIN, SYS_PTRACE, SYS_MODULE, DAC_READ_SEARCH, DAC_OVERRIDE). The denylist omitted CAP_SYS_TIME, among others. As a result, a tenant who could create a Function or Environment CRD could request securityContext.capabilities.add: ["SYS_TIME"], pass Fission's admission validation and merge-layer sanitization, and run attacker-controlled code with CAP_SYS_TIME in the resulting function or runtime container. This issue has been patched in version 1.25.0.	2026-06-10	8.5	CVE-2026-50570
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.24.0, Fission's buildermgr controller processed Package CRDs without verifying that Package.spec.environment.namespace matched Package.metadata.namespace. This issue has been patched in version 1.24.0.	2026-06-10	7.7	CVE-2026-49821
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.24.0, a low-privilege developer who could create a KubernetesWatchTrigger (KWT) in their own namespace was able to establish a persistent surveillance channel over any other namespace. This issue has been patched in version 1.24.0.	2026-06-10	7.7	CVE-2026-49822
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.24.0, a Fission Function spec carries three reference types - Secret, ConfigMap, and Package. The first two were namespace-validated by the admission webhook; PackageRef.Namespace was not. This issue has been patched in version 1.24.0.	2026-06-10	7.7	CVE-2026-49823

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.25.0, Unarchive in pkg/utls/zip.go joined each archive entry name with the destination directory via filepath.Join and wrote the result without checking whether the resolved path stayed under the destination. A zip entry named ../../tmp/evil therefore landed at /tmp/evil. An attacker who could control a Package.Spec.Source.URL or Deployment.URL archive could induce the fetcher (running as the per-environment pod's fission-fetcher sidecar) to write files anywhere that process could reach: into other tenants' /packages/<ns>/ directories, into mounted secret/config volumes, or into the fetcher's own binary. This issue has been patched in version 1.25.0.	2026-06-10	7.7	CVE-2026-50567
Flux159--mcp-server-kubernetes	mcp-server-kubernetes is a Model Context Protocol server for Kubernetes cluster management. Prior to version 3.6.0, mcp-server-kubernetes exposes three environment variables (ALLOW_ONLY_READONLY_TOOLS, ALLOW_ONLY_NON_DESTRUCTIVE_TOOLS, ALLOWED_TOOLS) documented as access controls for restricting which Kubernetes operations are available. These controls are enforced at the tool discovery layer (tools/list) but not at the execution layer (tools/call). Any client that knows a tool name can invoke it directly regardless of the configured restriction mode. The access control was effectively cosmetic. This issue has been patched in version 3.6.0.	2026-06-11	8.8	CVE-2026-46519
foliovision--FV Flowplayer Video Player	The FV Flowplayer Video Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the comment text in all versions up to, and including, 7.5.49.7212 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires an administrator to have enabled the non-default 'Parse Vimeo and YouTube links' (parse_comments) plugin setting, and requires a submitted comment to be approved by an administrator before the payload is publicly delivered.	2026-06-09	7.2	CVE-2026-7556
form-data--form-data	form-data is a library for creating readable multipart/form-data streams. In versions through 4.0.5, the 'field' argument to 'FormData#append' and the 'filename' option are concatenated verbatim into the 'Content-Disposition' header without escaping carriage return (CR), line feed (LF), or double-quote (") characters. An application that passes attacker-controlled data as a field name or filename (for example, an API gateway that turns JSON object keys into multipart field names) allows the attacker to terminate the header line and inject additional headers, or to smuggle entire additional multipart parts, into the request the application forwards to a backend. This can let the attacker add or override form fields (e.g. set 'is_admin=true') seen by the downstream parser. This is an instance of CWE-93 (CRLF injection). The fix escapes CR, LF, and '"' as '%0D', '%0A', and '%22' in field names and filenames, matching the serialization browsers use per the WHATWG HTML multipart/form-data encoding algorithm. Exploitation requires the consuming application to use untrusted input as a field name or filename; applications that use only fixed/trusted field names are not affected. Fixed in 2.5.6, 3.0.5, and 4.0.6.	2026-06-12	7.5	CVE-2026-12143
Fortinet--FortiSandbox	A improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.5, FortiSandbox 4.4.0 through 4.4.8, FortiSandbox 4.2 all versions, FortiSandbox Cloud 5.0.4 through 5.0.5, FortiSandbox PaaS 5.0.4 through 5.0.5 may allow an unauthenticated attacker to execute unauthorized commands via specifically crafted HTTP requests	2026-06-09	9.1	CVE-2026-25089
GALAYOU--Y4	A vulnerability was determined in GALAYOU Y4 1.0.0. Impacted is an unknown function of the component Web Server. This manipulation causes buffer overflow. The attack is only possible within the local network. The exploit has been publicly disclosed and may be utilized. The	2026-06-14	8.8	CVE-2026-12192

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vendor was contacted early about this disclosure but did not respond in any way.			
garlic-signage-- garlic-hub	Garlic-Hub manages digital signage network - devices, content, and playlists - from a single self-hosted interface. Prior to version 1.1, authenticated users can cause the server to issue arbitrary HTTP requests to internal services via the uploadFromUrl endpoint. This allows internal port scanning, service fingerprinting, and retrieval of internal HTTP responses which are stored in the publicly accessible media pool. This issue has been patched in version 1.1.	2026-06-11	7.7	CVE-2026-47170
Gen Digital-- Avast Antivirus	Heap buffer out-of-bounds write vulnerability in Avast Antivirus when scanning a malformed Windows PE file may allow Local Execution of Code or Denial-of-Service of the antivirus process. This issue affects Avast Antivirus, AVG Antivirus, Norton Antivirus, Avast One, and Avast Business Antivirus on Windows, macOS, and Linux for virus definition builds before VPS 25040308. The affected scanning logic is delivered through a shared Gen Digital virus definition update stream. The same stream feeds the consumer antivirus products listed in this advisory and other Gen Digital products that embed the same engine. Mitigation flows through this update channel; installations at or above the listed build are not vulnerable regardless of which product consumes the stream.	2026-06-12	7.8	CVE-2025-7004
Gen Digital-- Avast Antivirus	Heap buffer out-of-bounds read vulnerability in Avast Antivirus when scanning a malformed Windows PE file with .NET metadata may allow Local Execution of Code or Denial-of-Service of the antivirus process. This issue affects Avast Antivirus, AVG Antivirus, Norton Antivirus, Avast One, and Avast Business Antivirus on Windows, macOS, and Linux for virus definition builds before VPS 25021310. The affected scanning logic is delivered through a shared Gen Digital virus definition update stream. The same stream feeds the consumer antivirus products listed in this advisory and other Gen Digital products that embed the same engine. Mitigation flows through this update channel; installations at or above the listed build are not vulnerable regardless of which product consumes the stream.	2026-06-12	7.8	CVE-2025-7008
Gen Digital-- Avast Antivirus	Heap buffer out-of-bounds read vulnerability in Avast Antivirus when scanning a malformed Windows PE file may allow Local Execution of Code or Denial-of-Service of the antivirus process. This issue affects Avast Antivirus, AVG Antivirus, Norton Antivirus, Avast One, and Avast Business Antivirus on Windows, macOS, and Linux for virus definition builds before VPS 25021310. The affected scanning logic is delivered through a shared Gen Digital virus definition update stream. The same stream feeds the consumer antivirus products listed in this advisory and other Gen Digital products that embed the same engine. Mitigation flows through this update channel; installations at or above the listed build are not vulnerable regardless of which product consumes the stream.	2026-06-12	7.8	CVE-2025-7009
Gen Digital-- Avast Antivirus	Heap out-of-bounds read vulnerability in Avast Antivirus when scanning a malformed zip file containing XML may allow Local Execution of Code or Denial-of-Service of the antivirus process. This issue affects Avast Antivirus, AVG Antivirus, Norton Antivirus, Avast One, and Avast Business Antivirus on Windows, macOS, and Linux for virus definition builds from 25020100 before 25021208. The affected scanning logic is delivered through a shared Gen Digital virus definition update stream. The same stream feeds the consumer antivirus products listed in this advisory and other Gen Digital products that embed the same engine. Mitigation flows through this update channel; installations at or above the listed build are not vulnerable regardless of which product consumes the stream.	2026-06-12	7.8	CVE-2025-7011
Gen Digital-- Avira Antivirus	Heap buffer out-of-bounds write vulnerability due to integer overflow in Avira Antivirus engine when scanning a malformed MS-DOS executable file may allow Local Execution of Code or Denial-of-Service of the antivirus engine process. This issue affects Avira Antivirus on Windows, macOS, and Linux for engine builds before 8.3.70.104.	2026-06-12	7.8	CVE-2025-14098

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Gen Digital--Avira Antivirus	Heap buffer out-of-bounds read vulnerability in Avira Antivirus engine when scanning a malformed PDF file may allow Local Execution of Code or Denial-of-Service of the antivirus engine process. This issue affects Avira Antivirus on Windows, macOS, and Linux for engine builds before 8.3.70.68.	2026-06-12	7.8	CVE-2025-7002
Gen Digital--Avira Antivirus	Heap buffer out-of-bounds read vulnerability in Avira Antivirus engine when scanning a malformed PDF file may allow Local Execution of Code or Denial-of-Service of the antivirus engine process. This issue affects Avira Antivirus on Windows, macOS, and Linux for engine builds before 8.3.70.56.	2026-06-12	7.8	CVE-2025-7003
Gen Digital--Avira Antivirus	Heap buffer out-of-bounds read vulnerability in Avira Antivirus engine when scanning a malformed Windows MSI file may allow Local Execution of Code or Denial-of-Service of the antivirus engine process. This issue affects Avira Antivirus on Windows, macOS, and Linux for engine builds before 8.3.70.56.	2026-06-12	7.8	CVE-2025-7017
Gen Digital--Avira Antivirus	Heap buffer out-of-bounds read vulnerability in Avira Antivirus engine when scanning a malformed Windows PE file may allow Local Execution of Code or Denial-of-Service of the antivirus engine process. This issue affects Avira Antivirus on Windows, macOS, and Linux for engine builds before 8.3.70.98.	2026-06-12	7.8	CVE-2025-9032
Gen Digital--Avira Antivirus	Heap buffer out-of-bounds read vulnerability in Avira Antivirus engine when scanning a malformed PDF file may allow Local Execution of Code or Denial-of-Service of the antivirus engine process. This issue affects Avira Antivirus on Windows, macOS, and Linux for engine builds before 8.3.70.76.	2026-06-12	7.8	CVE-2025-9033
Gen Digital--Avira Antivirus	Heap buffer out-of-bounds write vulnerability in Avira Antivirus engine when scanning a malformed POSIX tar archive may allow Local Execution of Code or Denial-of-Service of the antivirus engine process. This issue affects Avira Antivirus on Windows, macOS, and Linux for engine builds before 8.3.27.12.	2026-06-12	7.8	CVE-2026-6676
Gen Digital--Avira Password Manager	Information disclosure vulnerability in Avira Password Manager when used with Mozilla Firefox may allow a remote attacker operating a cross-origin iframe to obtain credentials autofilled for the parent web page via incorrect autofill field selection. This issue affects Avira Password Manager when used with Mozilla Firefox on Windows, macOS, and Linux.	2026-06-12	7.4	CVE-2026-12068
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 17.1 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2 that under certain conditions could have allowed an authenticated user with developer-role permissions to execute arbitrary client-side code on behalf of a targeted user due to improper input sanitization in the Analytics Dashboard.	2026-06-11	8.7	CVE-2026-10087
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 15.5 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2 that under certain conditions could have allowed an authenticated user with group Owner role to take over another group member's GitLab account due to improper authorization in the Group SAML identity management functionality.	2026-06-11	8.7	CVE-2026-6552
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.10 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2 that under certain conditions could have allowed an unauthenticated user to cause denial of service due to improper input validation in the API request parsing middleware.	2026-06-11	7.5	CVE-2026-7250
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 13.1.4 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2 that under certain conditions could have allowed an authenticated user to add unauthorized email addresses to a targeted user's account due to improper sanitization of user-supplied input in certain group setting fields.	2026-06-11	7.3	CVE-2026-8589
GL.iNet--GL-MT3000	A weakness has been identified in GL.iNet GL-MT3000 up to 4.4.5. Affected is the function replace_country in the library /usr/lib/oui-httpd/rpc/tor of	2026-06-14	8.8	CVE-2026-12186

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the component Tor Proxy Service Configuration Handler. This manipulation causes command injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 4.7 is able to address this issue. It is recommended to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.			
GL.iNet--GL-MT3000	A security vulnerability has been detected in GL.iNet GL-MT3000 up to 4.4.5. Affected by this vulnerability is an unknown functionality of the file /usr/bin/one_click_upgrade of the component Online Firmware Upgrade Handler. Such manipulation leads to command injection. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 4.7 addresses this issue. Upgrading the affected component is advised. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	2026-06-14	8.8	CVE-2026-12187
Global IT Informatics Services Inc.--WEOLL	Unrestricted upload of file with dangerous type vulnerability in Global IT Informatics Services Inc. WEOLL allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects WEOLL: from 2.0.9 before 3.2.45.33.	2026-06-12	8.7	CVE-2026-6211
grobakability--snipe-it	Snipe-IT is an IT asset/license management system. A vulnerability in versions prior to 8.6.0 allows a non-admin user holding only the granular `users.edit` permission to lock every admin out of the instance by editing the `activated` flag (which determines whether or not a user can login) and the `ldap_import` flag, which determines whether or not the user can request a password reset. Version 8.6.0 contains a patch.	2026-06-08	7.1	CVE-2026-48507
Hippoo--Hippoo Mobile App for WooCommerce	Incorrect Privilege Assignment vulnerability in Hippoo Mobile App for WooCommerce allows Privilege Escalation. This issue affects Hippoo Mobile App for WooCommerce: from n/a through 1.9.4.	2026-06-11	9.8	CVE-2026-49060
IBM--i	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a user to gain elevated privileges due to an unqualified library call. A malicious actor could cause user-controlled code to run with administrator privilege.	2026-06-11	8.8	CVE-2026-7870
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.9.1 could allow an authenticated user to read or modify sensitive information by bypassing authentication using insecure direct object references.	2026-06-11	7.5	CVE-2026-7787
IBM--Qiskit SDK	IBM Qiskit SDK 0.43.0 through 2.5.0 could allow an attacker to trigger a segmentation fault leading to a denial of service due to uncontrolled recursion in the parser.	2026-06-12	7.5	CVE-2026-4870
IEI Integration Corp--iRM-TSi410X	The iRM-IEI Remote Management developed by IEI Integration Corp has a Hardcoded Credentials vulnerability, allowing unauthenticated remote attackers to exploit hard-coded credentials to gain administrative privileges on the database.	2026-06-12	9.8	CVE-2026-11849
IEI Integration Corp--iVEC TANK-XM811	The iVEC-IEI Virtualization Edge Computer developed by IEI Integration Corp has an Arbitrary File Deletion vulnerability, allowing authenticated remote attackers to exploit this vulnerability to delete arbitrary system files or directories, resulting in data destruction or service disruption.	2026-06-12	8.1	CVE-2026-11846
IEI Integration Corp--iVEC TANK-XM811	The iVEC-IEI Virtualization Edge Computer developed by IEI Integration Corp has a OS Command Injection vulnerability, allowing privileged remote attackers to inject arbitrary OS commands and execute them on the device.	2026-06-12	7.2	CVE-2026-11845
image-size--image-size	image-size through 2.0.2 contains a denial of service vulnerability that allows remote attackers to permanently block the Node.js event loop by supplying a specially crafted image buffer with a zero-valued size field in a recognized box-type. Attackers can trigger an infinite loop in the JXL or HEIF image parsers by providing a crafted image containing a box with a size of zero, causing the offset to never advance and permanently hanging the application.	2026-06-09	7.5	CVE-2025-71319
image-size--image-size	image-size through 2.0.2 contains a denial of service vulnerability that allows remote attackers to permanently block the Node.js event loop by	2026-06-10	7.5	CVE-2025-71329

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	supplying a specially crafted image buffer with a zero-valued size field in a recognized box-type. Attackers can trigger an infinite loop in the JXL or HEIF image parsers by providing a crafted image containing a box with a size of zero, causing the offset to never advance and permanently hanging the application.			
image-size-- image-size	image-size through 2.0.2 contains a denial of service vulnerability that allows remote attackers to permanently block the Node.js event loop by supplying a specially crafted ICNS image buffer. Attackers can craft an ICNS buffer containing valid magic bytes and a zero-valued entry length field to trigger an infinite loop in the ICNS parser, as the offset is never incremented when the entry length field is 0, causing the while loop condition to remain true indefinitely.	2026-06-10	7.5	CVE-2025-71330
ImageMagick-- ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-48 and 7.1.2-23, when reading multiple images with different dimensions an out of bounds heap write can occur. This issue has been patched in versions 6.9.13-48 and 7.1.2-23.	2026-06-10	7.5	CVE-2026-46520
ImageMagick-- ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2.23 and 6.9.13-48, due to a missing check in the MIFF decoder, a crafted file could cause an infinite loop resulting in CPU exhaustion. Versions 7.1.2.23 and 6.9.13-48 fix the issue.	2026-06-10	7.5	CVE-2026-46522
ImageMagick-- ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-48 and 7.1.2-24, a missing check in the DCM decoder could result in an image with invalid dimensions and that could cause crashes in other operation. This issue has been patched in versions 6.9.13-48 and 7.1.2-24.	2026-06-10	7.5	CVE-2026-49218
ImageMagick-- ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-50 and 7.1.2-25, a missing check for maximum memory request in AcquireAlignedMemory could trigger an out-of-Memory condition. This issue has been patched in versions 6.9.13-50 and 7.1.2-25.	2026-06-10	7.5	CVE-2026-53460
ImageMagick-- ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-50 and 7.1.2-25, an incorrect loop in the ICON decoder can result in an out of bounds heap write resulting in a crash. This issue has been patched in versions 6.9.13-50 and 7.1.2-25.	2026-06-10	7.5	CVE-2026-53461
imvks786-- student_management_system	A vulnerability was identified in imvks786 student_management_system up to 9599b560ad3c3b83e75d328b76bedcd489ef1f46. This affects an unknown function of the file /index.ph of the component Login. Such manipulation of the argument usr/pwd leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-08	7.3	CVE-2026-11530
imvks786-- student_management_system	A security flaw has been discovered in imvks786 student_management_system up to 9599b560ad3c3b83e75d328b76bedcd489ef1f46. This impacts an unknown function of the file admin/admin_login.php of the component Administrator Login Endpoint. Performing a manipulation of the argument a_usr/a_pwd results in sql injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-08	7.3	CVE-2026-11531
Inisev--Copy & Delete Posts	Copy & Delete Posts through 1.5.4 lets any plugin-enabled non-admin role invoke every operation in the cdp_action_handling AJAX handler.	2026-06-10	8.1	CVE-2026-53738

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Attackers with an enabled role can delete posts or overwrite plugin settings via the f parameter, bypassing per-function capability checks.			
InternLM--lmdeploy	LMDeploy is a toolkit for compressing, deploying, and serving large language models. In versions 0.12.3 and prior, LMDeploy is vulnerable to arbitrary code execution through hardcoded "trust_remote_code=True" in multiple HuggingFace model-loading call sites. At time of publication, there are no publicly available patches.	2026-06-09	7.8	CVE-2026-46432
InternLM--lmdeploy	LMDeploy is a toolkit for compressing, deploying, and serving large language models. In versions 0.12.3 and prior, hardcoded "trust_remote_code=True" enables HF supply-chain RCE without user opt-in. At time of publication, there are no publicly available patches.	2026-06-09	7.8	CVE-2026-46517
iova.mihai--SliceWP	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in iova.Mihai SliceWP allows Stored XSS. This issue affects SliceWP: from n/a through 1.2.6.	2026-06-11	7.1	CVE-2026-42653
Ivanti--Endpoint Manager Mobile	An OS command injection vulnerability in Ivanti EPMM before 12.9.0.1, 12.8.0.3 and 12.7.0.2 versions allows a remote authenticated attacker to execute arbitrary commands as root	2026-06-09	7.2	CVE-2026-10727
Ivanti--Sentry	An OS Command Injection vulnerability in Ivanti Sentry before the R10.5.2, R10.6.2 and R10.7.1 versions allows a remote unauthenticated user to achieve root-level remote code execution	2026-06-09	10	CVE-2026-10520
Ivanti--Sentry	An Authentication Bypass vulnerability (CWE-288) in Ivanti Sentry before the R10.5.2, R10.6.2 and R10.7.1 versions allows a remote unauthenticated attacker to create arbitrary administrative accounts and obtain full administrative access	2026-06-09	9.9	CVE-2026-10523
jelmer--dulwich	Dulwich is a pure-Python implementation of the Git file formats and protocols. Versions starting with 0.10.0 and prior to 1.2.5 have an arbitrary file write leading to remote code execution when cloning or checking out a malicious Git repository on Windows. Dulwich's path-element validator accepted tree entries whose filenames contained bytes that Windows interprets as structural path syntax. Contributing configuration bugs made matters worse. The core.protectNTFS and core.protectHFS settings were looked up under a wrong option name and so user-set values were silently ignored, and core.protectNTFS only defaulted to true on Windows (Git upstream has defaulted it to true everywhere since CVE-2019-1353). Both have been corrected. Anyone who clones, fetches, or checks out an untrusted repository with Dulwich on Windows - either through the Dulwich CLI, porcelain.clone, or any downstream tool built on Dulwich - is impacted. POSIX clones are not directly exploitable (on POSIX \ is a literal filename byte), but a POSIX user can unknowingly propagate a malicious tree to Windows consumers via push or re-publication. This issue is fixed in Dulwich 1.2.5. Users should upgrade to 1.2.5 or later. There is no effective pre-patch workaround. On affected versions the core.protectNTFS configuration key was silently ignored, so setting it to true does not mitigate the issue. Users who cannot upgrade should avoid cloning, fetching, or checking out untrusted repositories with Dulwich on Windows. After upgrading the NTFS validator is on by default on every platform, so no additional configuration is required.	2026-06-10	8.8	CVE-2026-42305
jelmer--dulwich	Dulwich is a pure-Python implementation of the Git file formats and protocols. Starting in version 0.23.2 and prior to version 1.2.5, `dulwich.porcelain.submodule_update`, and by extension `porcelain.clone(..., recurse_submodules=True)`, materializes attacker-controlled submodule paths from a crafted upstream repository without path validation. A malicious `.gitmodules` plus a matching tree gitlink whose `path` is `.git/hooks` (or any other directory inside the parent repository's `.git` directory) causes the attacker's submodule tree contents to be written directly into the victim's `.git/hooks/` directory, preserving executable mode bits. The dropped executables are then run by any subsequent `git` or `dulwich` command that invokes the matching hook, resulting in arbitrary code execution. This is the dulwich equivalent of the	2026-06-10	7.5	CVE-2026-52726

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	upstream Git fixes for CVE-2024-32002 / CVE-2024-32004, which were never propagated into dulwich's separately implemented submodule porcelain. Version 1.2.5 patches the issue.			
jmespath--jmespath.php	jmespath.php allows users to use JMESPath, software for declaratively specifying how to extract elements from a JSON document, in PHP applications with PHP data structures. Versions prior to 2.9.1 can generate and execute attacker-controlled PHP code when `JmesPath\CompilerRuntime` is used with an attacker-controlled JMESPath expression. The compiler emits parsed JMESPath function names into generated PHP source without sufficient escaping. A crafted expression can cause the generated cache file to contain executable attacker-controlled PHP, which is then loaded by the compiler runtime. The issue is patched in `2.9.1` and later. As a workaround, disable `JP_PHP_COMPILE` and do not use `JmesPath\CompilerRuntime` with attacker-controlled expressions. Use the default `AstRuntime` for untrusted expressions. Applications that must continue accepting untrusted JMESPath expressions before upgrading should ensure those expressions are never evaluated by the compiler runtime.	2026-06-12	9.8	CVE-2026-54133
john-dagelmore-GPTranslate Multilingual AI Translation for WordPress: Automatically Translate Websites	The GPTranslate - Multilingual AI Translation for WordPress: Automatically Translate Websites plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REST API Translation Storage in all versions up to, and including, 2.31 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The deterministically derived API key (sha256 of the site URL) is printed in the HTML source of every page via the JavaScript variable gptApiKey, meaning any unauthenticated visitor can retrieve the key and submit malicious translation payloads to the /wp-json/gptranslate/v1/request endpoint without any additional precondition.	2026-06-13	7.2	CVE-2026-9109
js-cookie--js-cookie	JavaScript Cookie is a JavaScript API for handling cookies, client-side. Prior to version 3.0.7, js-cookie's internal assign() helper copies properties with for...in + plain assignment. When the source object is produced by JSON.parse, the JSON object's "__proto__" member is an own enumerable property, so the for-in enumerates it and the target[key] = source[key] write triggers the Object.prototype.__proto__ setter on the fresh target ({}). The result is a per-instance prototype hijack: Object.prototype itself is untouched, but the merged attributes object now inherits attacker-controlled keys. Because the consuming set() function then enumerates the merged object with another for...in, every key the attacker placed on the polluted prototype lands in the resulting Set-Cookie string as an attribute pair. The attacker can set domain=, secure=, samesite=, expires=, and path= on cookies whose attributes the developer thought were locked down. This issue has been patched in version 3.0.7.	2026-06-10	7.5	CVE-2026-46625
koel--koel	Koel is a free, open-source music streaming solution. Prior to version 9.3.5, Koel validates the podcast feed URL via the SafeUrl rule (DNS resolution + public IP check), but the individual episode <enclosure url="..."> values extracted from the RSS XML are stored directly into the database without any SSRF validation. When a user plays an episode, the server downloads the full HTTP response from the unvalidated enclosure URL via Http::sink()->get() and streams it back to the user, enabling full-read SSRF against internal services. This issue has been patched in version 9.3.5.	2026-06-12	7.7	CVE-2026-47260
Koha Community--Koha	SQL Injection in reports/catalogue_out.pl in Koha Community Koha through 22.11.37, 23.x, 24.x before 24.11.16, 25.05.x before 25.05.11, 25.11.x before 25.11.05, 26.05.x before 26.05.01, and 26.11.x before 26.11.00 allows an authenticated staff user with the Reports module flag to read arbitrary data from the Koha application database via the Filter URL parameter when the Criteria parameter matches /branchcode/. The vulnerable sink in sub calculate concatenates the unmodified Filter request	2026-06-13	7.6	CVE-2026-6428

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	parameter directly into a LIKE clause of the auxiliary \$strsth2 statement and executes it via DBI without bound parameters: my \$f = @\$filters[0]; \$f =~ s/*/%/g; \$strsth2 .= " AND \$column LIKE '\$f' "; This enables error-based SQL injection (e.g., via EXTRACTVALUE) and full read access to sensitive tables including borrowers (password hashes, 2FA secrets, PII), borrower_password_recovery, api_keys, and sessions. Proof of concept (error-based, single request): GET /cgi-bin/koha/reports/catalogue_out.pl?do_it=1&output=screen&Limit=10&Criteria=branchcode&Filter=x'+AND+EXTRACTVALUE(1,CONCAT(0x7e,VERSION(),0x7c,USER(),0x7c,DATABASE(),0x7e))--+ Cookie: CGISESSID=<LIBRARIAN_SESSION> The response body contains the DBI exception leaking the MariaDB version, database user, client IP, and database name, after which arbitrary data can be paged out using LIMIT n,1 / SUBSTRING(...). The vulnerable sink was introduced in commit 6bb77ae3e4 (2008-07-09); CVE-2015-4633 patched the same class in sibling files but did not generalise the fix to reports/catalogue_out.pl. Fixed in Koha 22.11.38, 24.11.16, 25.05.11, 25.11.05, 26.05.01, and 26.11.00 by replacing the raw concatenation with a parameterised placeholder.			
kovidgoyal--kitty	Kitty is a cross-platform GPU based terminal. In versions prior to 0.47.0, a program able to write bytes to a kitty terminal - a remote SSH peer, a downloaded file viewed with `cat`, a log line, an email body rendered in `less`, an issue body in a TUI, etc. - can cause kitty to execute attacker-supplied Python inside the running kitty process, with the user's full privileges. There is no approval prompt, no remote-control permission requirement, no shell-integration interaction, no clipboard touch, and no editor interaction. Version 0.47.0 fixes the issue.	2026-06-12	7.8	CVE-2026-42851
kovidgoyal--kitty	Kitty is a cross-platform GPU based terminal. In versions 0.47.0 and 0.47.1, `kitten dnd` can allow a malicious remote drag-and-drop source to overwrite or truncate arbitrary files writable by the local kitty user. Remote `text/uri-list` drops are staged in a temporary directory, but on case-sensitive filesystems duplicate remote basenames are not de-duplicated. An attacker can first create a staged symlink and then send a same-name regular-file entry. The regular-file write uses `utils.CreateAt()` / `openat(O_RDWR O_CREAT O_TRUNC)` without `O_NOFOLLOW`, so it follows the attacker-created symlink and writes outside the staging directory before final overwrite confirmation runs. This appears related in class to the file-transfer symlink advisory, but it is a different bug: it affects `kitten dnd` remote drag-and-drop staging, uses different vulnerable code (`kittens/dnd/drop.go` and `tools/utils/file_at_fd.go`), and reproduces on commit `4aa4a5c0567a92553a8c20a88a4352da637fca5d`, after the file-transfer `O_NOFOLLOW` fix. Version 0.47.2 patches the issue.	2026-06-12	7.6	CVE-2026-54056
Kushan2k--student-management-system	A security flaw has been discovered in Kushan2k student-management-system up to f16a4ceadd6729c4b306ed4641cda3176c1ef2a. Affected is an unknown function of the file service/RegisterService.php of the component Registration Endpoint. Performing a manipulation of the argument sting results in unrestricted upload. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-08	7.3	CVE-2026-11474
ladela--Online Scheduling and Appointment Booking System Bookly	The Online Scheduling and Appointment Booking System - Bookly plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'bookly-customer-full-name' cookie in versions up to, and including, 27.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation	2026-06-13	7.2	CVE-2026-5513

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	requires 'Remember personal information in cookies' setting to be enabled (disabled by default).			
Lenovo--Accessories and Display Manager for Enterprise	During an internal security assessment, a potential vulnerability was discovered in Lenovo Accessories and Display Manager for Enterprise for Windows that could allow a local authenticated user to execute arbitrary code with elevated privileges.	2026-06-10	7.8	CVE-2026-9045
Lenovo--LanSchool Classic	A potential uncontrolled search path vulnerability was reported in the LanSchool Classic client application that could allow a local authenticated user to execute arbitrary code with elevated privileges.	2026-06-10	7.8	CVE-2026-8637
Lenovo--Smart Connect	A potential authentication bypass was reported in Lenovo Smart Connect for Windows that could allow a local authenticated user to execute arbitrary code with elevated privileges.	2026-06-10	7	CVE-2026-6090
LiamBindle--MQTT-C	LiamBindle MQTT-C through version 1.1.6 contains a heap-based out-of-bounds read and integer underflow in the mqtt_unpack_publish_response() function in src/mqtt.c that allows a remote unauthenticated attacker controlling an MQTT broker - or able to inject MQTT traffic into an unencrypted session - to crash a subscribed MQTT-C client and potentially disclose adjacent heap memory by sending a single crafted PUBLISH packet. The function validates only that the fixed-header remaining_length is at least 4, then reads the 16-bit topic_name_size field from the broker-controlled packet and advances the parse pointer by that value without verifying that topic_name_size plus the surrounding overhead fits within remaining_length; it subsequently computes application_message_size as remaining_length - topic_name_size - 2 (QoS 0) or - 4 (QoS greater than 0) in unsigned arithmetic, producing an integer underflow that is then passed to memmove(). A PUBLISH packet with topic_name_size = 0xFFFF and remaining_length = 7 advances the parse pointer 65535 bytes past the receive buffer (out-of-bounds read) and causes an application_message_size near 2^32, crashing the process when the resulting memmove() is executed.	2026-06-14	8.2	CVE-2026-54412
libp2p--js-libp2p	libp2p is a JavaScript Implementation of libp2p networking stack. Prior to version 16.2.6, an unauthenticated remote peer can exhaust the disk storage of any @libp2p/kad-dht node running in server mode by sending an unbounded stream of PUT_VALUE messages whose keys bypass all content validation. No credentials, no prior relationship, and no protocol deviation beyond a crafted key are required. The victim node's datastore fills until the host disk is exhausted, making the node unavailable. This issue has been patched in version 16.2.6.	2026-06-10	7.5	CVE-2026-45783
libp2p--js-libp2p	libp2p is a JavaScript Implementation of libp2p networking stack. Prior to version 15.0.23, three cooperating omissions in @libp2p/gossipsub allow an unauthenticated single peer to exhaust the Node.js heap of any gossipsub node with default options. This issue has been patched in version 15.0.23.	2026-06-10	7.5	CVE-2026-46679
Limetek System Inc.--LimRAD NAC	Unrestricted upload of file with dangerous type vulnerability in Limetek System Inc. LimRAD NAC allows Remote Code Inclusion. This issue affects LimRAD NAC: before 5.5.7.3.9.	2026-06-11	9.8	CVE-2026-7852
LimeSurvey--LimeSurvey	LimeSurvey constructs account password-reset links from the client-supplied HTTP Host header without validating it. The optional allowedHosts allowlist that would constrain this is undefined in the default (and documented) configuration, so LSHttpRequest::checkIsAllowedHost() results in no operation. A remote, unauthenticated attacker who submits a forgotten-password request for a known account (requiring only the target's username and email) with a spoofed Host header causes LimeSurvey to email that account a reset link whose hostname is attacker-controlled while embedding the genuine validation_key. When the recipient or an automated inbound mail-security link scanner dereferences the link, the valid reset token is disclosed to the attacker, who replays it	2026-06-09	8.8	CVE-2026-50635

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	against the legitimate host's newPassword endpoint to set a new password and take over the account.			
LimeSurvey--LimeSurvey	The RemoteControl API methods invite_participants and remind_participants pass a caller-supplied token-ID array into TokenDynamic::findUninvited(), which concatenates the values directly into a tid IN ('...') SQL clause without parameterization or input validation. A remote, authenticated attacker holding the tokens/update permission on a survey can inject a crafted array element to perform SQL injection. Because LimeSurvey configures its PDO connection with emulated prepared statements (emulatePrepare = true) and does not disable MySQL multi-statements, the injection supports stacked queries: the attacker can append arbitrary additional statements (INSERT/UPDATE/DELETE/DROP/CREATE) after the original SELECT. This permits both arbitrary read of any data in the database, such as administrator bcrypt password hashes (lime_users), survey response PII, session records, and global settings, all recoverable via a SLEEP() time-based blind oracle, and arbitrary write/destruction of that data, including directly overwriting the administrator password hash for immediate account takeover or dropping/truncating tables. Reads and writes extend to any schema the application's database user can access. The RemoteControl interface (RPCInterface = json/xml) must be enabled, which is not the default.	2026-06-09	8.8	CVE-2026-50636
lingdojo--kana-dojo	KanaDojo before 0.1.18 contains a sandbox escape vulnerability that allows an attacker to execute arbitrary code by exploiting the explicit passing of the global require function into a Node.js vm.runInNewContext() sandbox context in the issue-auto-respond.yml workflow. Attackers can submit a pull request modifying messages.cjs to import arbitrary Node.js modules, bypassing sandbox restrictions and achieving remote code execution with full GitHub Actions runner privileges including access to AUTOMATION_PR_TOKEN.	2026-06-11	7.3	CVE-2026-48546
lingdojo--kana-dojo	KanaDojo contains a command injection vulnerability that allows an attacker with pull request access to execute arbitrary shell commands by inserting shell metacharacters into the version or changes fields of patchNotesData.json, which are interpolated unsanitized into a child_process.execSync() call in the release.yml workflow. Attackers can have a malicious pull request merged to trigger the GitHub Actions runner with contents write permissions and access to GITHUB_TOKEN.	2026-06-11	7.3	CVE-2026-48547
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: lib/scatterlist: fix length calculations in extract_kvec_to_sg Patch series "Fix bugs in extract_iter_to_sg()", v3. Fix bugs in the kvec and user variants of extract_iter_to_sg. This series is growing due to useful remarks made by sashiko.dev. The main bugs are: - The length for an sglist entry when extracting from a kvec can exceed the number of bytes in the page. This is obviously not intended. - When extracting a user buffer the sglist is temporarily used as a scratch buffer for extracted page pointers. If the sglist already contains some elements this scratch buffer could overlap with existing entries in the sglist. The series adds test cases to the kunit_iov_iter test that demonstrate all of these bugs. Additionally, there is a memory leak fix for the test itself. The bugs were originally introduced into kernel v6.3 where the function lived in fs/netfs/iterator.c. It was later moved to lib/scatterlist.c in v6.5. Thus the actual fix is only marked for backports to v6.5+. This patch (of 5): When extracting from a kvec to a scatterlist, do not cross page boundaries. The required length was already calculated but not used as intended. Adjust the copied length if the loop runs out of sglist entries without extracting everything. While there, return immediately from extract_iter_to_sg if there are no sglist entries at all. A subsequent commit will add kunit test cases that demonstrate that the patch is necessary.	2026-06-08	9.8	CVE-2026-46289

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: vgif-its: Drop the translation cache reference only for the erased entry vgif_its_invalidate_cache() walks the per-ITS translation cache with xa_for_each() and drops the cache's reference on each entry with vgif_put_irq(). It puts the iterated pointer, though, rather than the value returned by xa_erase(). The function is called from contexts that do not exclude one another: the ITS command handlers hold its_lock, the GITS_CTLR write path holds cmd_lock, and the path that clears EnableLPis in a redistributor's GICR_CTLR holds neither. Two or more of them can drain the same cache concurrently, and if each one observes the same entry, erases it and then puts it, the single reference the cache holds on that entry is dropped more than once. The entry can then be freed while an ITE still maps it. xa_erase() is atomic and returns the previous entry, so put only the entry that this context actually removed. The cache reference is then dropped exactly once per entry even when the invalidations run concurrently, and the behavior is unchanged when only one context runs.	2026-06-09	9.3	CVE-2026-46316
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/rxe: Fix iova-to-va conversion for MR page sizes != PAGE_SIZE The current implementation incorrectly handles memory regions (MRs) with page sizes different from the system PAGE_SIZE. The core issue is that rxe_set_page() is called with mr->page_size step increments, but the page_list stores individual struct page pointers, each representing PAGE_SIZE of memory. ib_sg_to_page() has ensured that when i>=1 either a) SG[i-1].dma_end and SG[i].dma_addr are contiguous or b) SG[i-1].dma_end and SG[i].dma_addr are mr->page_size aligned. This leads to incorrect iova-to-va conversion in scenarios: 1) page_size < PAGE_SIZE (e.g., MR: 4K, system: 64K): ibmr->iova = 0x181800 sg[0]: dma_addr=0x181800, len=0x800 sg[1]: dma_addr=0x173000, len=0x1000 Access iova = 0x181800 + 0x810 = 0x182010 Expected VA: 0x173010 (second SG, offset 0x10) Before fix: - index = (0x182010 >> 12) - (0x181800 >> 12) = 1 - page_offset = 0x182010 & 0xFFF = 0x10 - xarray[1] stores system page base 0x170000 - Resulting VA: 0x170000 + 0x10 = 0x170010 (wrong) 2) page_size > PAGE_SIZE (e.g., MR: 64K, system: 4K): ibmr->iova = 0x18f800 sg[0]: dma_addr=0x18f800, len=0x800 sg[1]: dma_addr=0x170000, len=0x1000 Access iova = 0x18f800 + 0x810 = 0x190010 Expected VA: 0x170010 (second SG, offset 0x10) Before fix: - index = (0x190010 >> 16) - (0x18f800 >> 16) = 1 - page_offset = 0x190010 & 0xFFFF = 0x10 - xarray[1] stores system page for dma_addr 0x170000 - Resulting VA: system page of 0x170000 + 0x10 = 0x170010 (wrong) Yi Zhang reported a kernel panic[1] years ago related to this defect. Solution: 1. Replace xarray with pre-allocated rxe_mr_page array for sequential indexing (all MR page indices are contiguous) 2. Each rxe_mr_page stores both struct page* and offset within the system page 3. Handle MR page_size != PAGE_SIZE relationships: - page_size > PAGE_SIZE: Split MR pages into multiple system pages - page_size <= PAGE_SIZE: Store offset within system page 4. Add boundary checks and compatibility validation This ensures correct iova-to-va conversion regardless of MR page size and system PAGE_SIZE relationship, while improving performance through array-based sequential access. Tests on 4K and 64K PAGE_SIZE hosts: - rdma-core/pytests \$./build/bin/run_tests.py --dev eth0_rxe - blktest: \$ TIMEOUT=30 QUICK_RUN=1 USE_RXE=1 NVMET_TRTYPES=rdma ./check_nvme srp rnbd [1] https://lore.kernel.org/all/CAHj4cs9XRqE25jyVw9rj9YugffLn5+f=1znaBEnu1usLOciD+g@mail.gmail.com/T/	2026-06-09	9.8	CVE-2026-46325
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: of: unittest: fix use-after-free in of_unittest_changese() The variable 'parent' is assigned the value of 'nchangeset' earlier in the function, meaning both point to the same struct device_node. The call to of_node_put(nchangeset) can decrement the reference count to zero and	2026-06-08	8.4	CVE-2026-46288

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	free the node if there are no other holders. After that, the code still uses 'parent' to check for the presence of a property and to read a string property, leading to a use-after-free. Fix this by moving the of_node_put() call after the last access to 'parent', avoiding the UAF.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: isofs: validate Rock Ridge CE continuation extent against volume size rock_continue() reads rs->cont_extent verbatim from the Rock Ridge CE record and passes it to sb_bread() without checking that the block number is within the mounted ISO 9660 volume. commit e595447e177b ("[PATCH] rock.c: handle corrupted directories") added cont_offset and cont_size rejection for the CE continuation but did not validate the extent block number itself. commit f54e18f1b831 ("isofs: Fix infinite looping over CE entries") later capped the CE chain length at RR_MAX_CE_ENTRIES = 32 but again left the block number unchecked. With a crafted ISO mounted via udisks2 (desktop optical auto-mount) or via CAP_SYS_ADMIN mount, rs->cont_extent can therefore point at an out-of-range block or at blocks belonging to an adjacent filesystem on the same block device. sb_bread() on an out-of-range block returns NULL cleanly via the block layer EIO path, so there is no memory-safety violation. For in-range reads of adjacent-filesystem data, the CE buffer is parsed as Rock Ridge records and only the text of SL sub-records reaches userspace through readlink(), which makes the info-leak channel narrow and difficult to exploit; still, rejecting the malformed CE outright matches the rejection shape already present in the same function for cont_offset and cont_size. Add an ISOFS_SB(sb)->s_nzones bounds check to rock_continue() next to the existing offset/size rejection, printing the same corrupted-directory-entry notice.	2026-06-08	8.2	CVE-2026-46303
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: ath5k: do not access array OOB Vincent reports: > The ath5k driver seems to do an array-index-out-of-bounds access as > shown by the UBSAN kernel message: > UBSAN: array-index-out-of-bounds in drivers/net/wireless/ath/ath5k/base.c:1741:20 > index 4 is out of range for type 'ieee80211_tx_rate [4]' > ... > Call Trace: > <TASK> > dump_stack_lvl+0x5d/0x80 > ubsan_epilogue+0x5/0x2b > __ubsan_handle_out_of_bounds.cold+0x46/0x4b > ath5k_tasklet_tx+0x4e0/0x560 [ath5k] > tasklet_action_common+0xb5/0x1c0 It is real. 'ts->ts_final_idx' can be 3 on 5212, so: info->status.rates[ts->ts_final_idx + 1].idx = -1; with the array defined as: struct ieee80211_tx_rate rates[IEEE80211_TX_MAX_RATES]; while the size is: #define IEEE80211_TX_MAX_RATES 4 is indeed bogus. Set this 'idx = -1' sentinel only if the array index is less than the array size. As mac80211 will not look at rates beyond the size (IEEE80211_TX_MAX_RATES). Note: The effect of the OOB write is negligible. It just overwrites the next member of info->status, i.e. ack_signal.	2026-06-08	8.3	CVE-2026-46307
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Reassign nested_mmus array behind mmu_lock kvm->arch.nested_mmus[] is walked under kvm->mmu_lock, including from the MMU notifier path (kvm_unmap_gfn_range() -> kvm_nested_s2_unmap()), which can run at any time. kvm_vcpu_init_nested() reallocates the array and frees the old buffer while holding only kvm->arch.config_lock, so such a walker can reference the freed array. Allocate the new array outside of mmu_lock, as the allocation can sleep. Under the lock, copy the existing entries, fix up the back pointers and reassign the array. Free the old buffer after dropping the lock, as kvfree() can sleep as well.	2026-06-09	8.8	CVE-2026-46317
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iio: pressure: mprls0025pa: fix spi_transfer struct initialisation Make sure that the spi_transfer struct is zeroed out before use.	2026-06-09	8.4	CVE-2026-46326

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: greybus: gb-beagleplay: bound bootloader receive buffering cc1352_bootloader_rx() appends each serdev chunk into the fixed rx_buffer before parsing bootloader packets. The helper can keep leftover bytes between callbacks and may receive multiple packets in one callback, so a single count value is not constrained by one packet length. Check that the incoming chunk fits in the remaining receive buffer space before memcpy(). If it does not, drop the staged data and consume the bytes instead of overflowing rx_buffer.	2026-06-09	8	CVE-2026-46332
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: io-wq: check that the predecessor is hashed in io_wq_remove_pending() io_wq_remove_pending() needs to fix up wq->hash_tail[] if the cancelled work was the tail of its hash bucket. When doing this, it checks whether the preceding entry in acct->work_list has the same hash value, but never checks that the predecessor is hashed at all. io_get_work_hash() is simply atomic_read(&work->flags) >> IO_WQ_HASH_SHIFT, and the hash bits are never set for non-hashed work, so it returns 0. Thus, when a hashed bucket-0 work is cancelled while a non-hashed work is its list predecessor, the check spuriously passes and a pointer to the non-hashed io_kiocb is stored in wq->hash_tail[0]. Because non-hashed work is dequeued via the fast path in io_get_next_work(), which never touches hash_tail[], the stale pointer is never cleared. Therefore, after the non-hashed io_kiocb completes and is freed back to req_cachep, wq->hash_tail[0] is a dangling pointer. The io_wq is per-task (tctx->io_wq) and survives ring open/close, so the dangling pointer persists for the lifetime of the task; the next hashed bucket-0 enqueue dereferences it in io_wq_insert_work() and wq_list_add_after() writes through freed memory. Add the missing io_wq_is_hashed() check so a non-hashed predecessor never inherits a hash_tail[] slot.	2026-06-08	7.8	CVE-2026-46274
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_uart: fix UAFs and race conditions in close and init paths Vulnerabilities leading to Use-After-Free (UAF) and Null Pointer Dereference (NPD) conditions were observed in the lifecycle management of hci_uart. The primary issue arises because the workqueues (init_ready and write_work) are only flushed/cancelled if the HCI_UART_PROTO_READY flag is set during TTY close. If a hangup occurs before setup completes, hci_uart_tty_close() skips the teardown of these workqueues and proceeds to free the `hu` struct. When the scheduled work executes later, it blindly dereferences the freed `hu` struct. Furthermore, several data races and UAFs were identified in the teardown sequence: 1. Calling hci_uart_flush() from hci_uart_close() without effectively disabling write_work causes a race condition where both can concurrently double-free hu->tx_skb. This happens because protocol timers can concurrently invoke hci_uart_tx_wakeup() and requeue write_work. 2. Calling hci_free_dev(hdev) before hu->proto->close(hu) causes a UAF when vendor specific protocol close callbacks dereference hu->hdev. 3. In the initialization error paths, failing to take the proto_lock write lock before clearing PROTO_READY leads to races with active readers. Additionally, hci_uart_tty_receive() accesses hu->hdev outside the read lock, leading to UAFs if the initialization error path frees hdev concurrently. Fix these synchronization and lifecycle issues by: 1. Re-ordering hci_uart_tty_close() to clear HCI_UART_PROTO_READY first, followed immediately by a cancel_work_sync(&hu->write_work). Clearing the flag locks out concurrent protocol timers from successfully invoking hci_uart_tx_wakeup(), effectively rendering the cancellation permanent and preventing the tx_skb double-free. 2. Note: Clearing PROTO_READY early causes hci_uart_close() to skip hu->proto->flush(). This is perfectly safe in the tty_close path because hu->proto->close() executes shortly after, which intrinsically purges all protocol SKB queues and tears down	2026-06-08	7.8	CVE-2026-46275

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the state. 3. Relocating hu->proto->close(hu) strictly prior to hci_free_dev(hdev) across all close and error paths to prevent vendor-level UAFs. 4. Moving the hdev->stat.byte_rx increment in hci_uart_tty_receive() inside the proto_lock read-side critical section to safely synchronize with device unregistration. 5. Adding cancel_work_sync(&hu->write_work) to hci_uart_close() to safely flush the workqueue before hci_uart_flush() is invoked via the HCI core. 6. Utilizing cancel_work_sync() instead of disable_work_sync() across all paths to prevent permanently breaking user-space retry capabilities.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mm/zone_device: do not touch device folio after calling ->folio_free() The contents of a device folio can immediately change after calling ->folio_free(), as the folio may be reallocated by a driver with a different order. Instead of touching the folio again to extract the pgmap, use the local stack variable when calling percpu_ref_put_many().	2026-06-08	7.8	CVE-2026-46277
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: lib: test_hmm: evict device pages on file close to avoid use-after-free Patch series "Minor hmm_test fixes and cleanups". Two bugfixes a cleanup for the HMM kernel selftests. These were mostly reported by Zenghui Yu with special thanks to Lorenzo for analysing and pointing out the problems. This patch (of 3): When dmirror_fops_release() is called it frees the dmirror struct but doesn't migrate device private pages back to system memory first. This leaves those pages with a dangling zone_device_data pointer to the freed dmirror. If a subsequent fault occurs on those pages (eg. during coredump) the dmirror_devmem_fault() callback dereferences the stale pointer causing a kernel panic. This was reported [1] when running mm/ksft_hmm.sh on arm64, where a test failure triggered SIGABRT and the resulting coredump walked the VMAs faulting in the stale device private pages. Fix this by calling dmirror_device_evict_chunk() for each devmem chunk in dmirror_fops_release() to migrate all device private pages back to system memory before freeing the dmirror struct. The function is moved earlier in the file to avoid a forward declaration.	2026-06-08	7.8	CVE-2026-46280
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: hfsplus: fix held lock freed on hfsplus_fill_super() hfsplus_fill_super() calls hfs_find_init() to initialize a search structure, which acquires tree->tree_lock. If the subsequent call to hfsplus_cat_build_key() fails, the function jumps to the out_put_root error label without releasing the lock. The later cleanup path then frees the tree data structure with the lock still held, triggering a held lock freed warning. Fix this by adding the missing hfs_find_exit(&fd) call before jumping to the out_put_root error label. This ensures that tree->tree_lock is properly released on the error path. The bug was originally detected on v6.13-rc1 using an experimental static analysis tool we are developing, and we have verified that the issue persists in the latest mainline kernel. The tool is specifically designed to detect memory management issues. It is currently under active development and not yet publicly available. We confirmed the bug by runtime testing under QEMU with x86_64 defconfig, lockdep enabled, and CONFIG_HFSPLUS_FS=y. To trigger the error path, we used GDB to dynamically shrink the max_unistr_len parameter to 1 before hfsplus_asc2uni() is called. This forces hfsplus_asc2uni() to naturally return -ENAMETOOLONG, which propagates to hfsplus_cat_build_key() and exercises the faulty error path. The following warning was observed during mount: ===== WARNING: held lock freed! 7.0.0-rc3-00016-gb4f0dd314b39 #4 Not tainted ----- mount/174 is freeing memory ffff888103f92000-ffff888103f92fff, with a lock still held there! ffff888103f920b0 (&tree->tree_lock){+.+.}-{4:4}, at: hfsplus_find_init+0x154/0x1e0 2 locks held by mount/174: #0: ffff888103f960e0 (&type->s_umount_key#42/1){+.+.}-{4:4}, at: alloc_super.constprop.0+0x167/0xa40 #1: ffff888103f920b0 (&tree-	2026-06-08	7	CVE-2026-46299

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	>tree_lock){+.+.}-{4:4}, at: hfsplus_find_init+0x154/0x1e0 stack backtrace: CPU: 2 UID: 0 PID: 174 Comm: mount Not tainted 7.0.0-rc3-00016-gb4f0dd314b39 #4 PREEMPT(lazy) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.15.0-1 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x82/0xd0 debug_check_no_locks_freed+0x13a/0x180 kfree+0x16b/0x510 ? hfsplus_fill_super+0xcb4/0x18a0 hfsplus_fill_super+0xcb4/0x18a0 ? __pfx_hfsplus_fill_super+0x10/0x10 ? srso_return_thunk+0x5/0x5f ? bdev_open+0x65f/0xc30 ? srso_return_thunk+0x5/0x5f ? pointer+0x4ce/0xbf0 ? trace_contention_end+0x11c/0x150 ? __pfx_pointer+0x10/0x10 ? srso_return_thunk+0x5/0x5f ? bdev_open+0x79b/0xc30 ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? vsnprintf+0x6da/0x1270 ? srso_return_thunk+0x5/0x5f ? __mutex_unlock_slowpath+0x157/0x740 ? __pfx_vsnprintf+0x10/0x10 ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? mark_held_locks+0x49/0x80 ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? irqentry_exit+0x17b/0x5e0 ? trace_irq_disable.constprop.0+0x116/0x150 ? __pfx_hfsplus_fill_super+0x10/0x10 ? __pfx_hfsplus_fill_super+0x10/0x10 get_tree_bdev_flags+0x302/0x580 ? __pfx_get_tree_bdev_flags+0x10/0x10 ? vfs_parse_fs_qstr+0x129/0x1a0 ? __pfx_vfs_parse_fs_qstr+0x3/0x10 vfs_get_tree+0x89/0x320 fc_mount+0x10/0x1d0 path_mount+0x5c5/0x21c0 ? __pfx_path_mount+0x10/0x10 ? trace_irq_enable.constprop.0+0x116/0x150 ? trace_irq_enable.constprop.0+0x116/0x150 ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? kmem_cache_free+0x307/0x540 ? user_path_at+0x51/0x60 ? __x64_sys_mount+0x212/0x280 ? srso_return_thunk+0x5/0x5f __x64_sys_mount+0x212/0x280 ? __pfx__x64_sys_mount+0x10/0x10 ? srso_return_thunk+0x5/0x5f ? trace_irq_enable.constprop.0+0x116/0x150 ? srso_return_thunk+0x5/0x5f do_syscall_64+0x111/0x680 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7ffacac55eae Code: 48 8b 0d 85 1f 0f 00 f7 d8 64 89 01 48 83 c8 ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 49 89 ca b8 a5 00 00 8 RSP: 002b ---truncated---			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nvmet: avoid recursive nvmet-wq flush in nvmet_ctrl_free nvmet_tcp_release_queue_work() runs on nvmet-wq and can drop the final controller reference through nvmet_cq_put(). If that triggers nvmet_ctrl_free(), the teardown path flushes ctrl->async_event_work on the same nvmet-wq. Call chain: nvmet_tcp_schedule_release_queue() kref_put(&queue->kref, nvmet_tcp_release_queue) nvmet_tcp_release_queue() queue_work(nvmet_wq, &queue->release_work) <--- nvmet_wq process_one_work() nvmet_tcp_release_queue_work() nvmet_cq_put(&queue->nvme_cq) nvmet_cq_destroy() nvmet_ctrl_put(cq->ctrl) nvmet_ctrl_free() flush_work(&ctrl->async_event_work) <--- nvmet_wq Previously Scheduled by :- nvmet_add_async_event queue_work(nvmet_wq, &ctrl->async_event_work); This trips lockdep with a possible recursive locking warning. [5223.015876] run blktests nvme/003 at 2026-04-07 20:53:55 [5223.061801] loop0: detected capacity change from 0 to 2097152 [5223.072206] nvmet: adding nsid 1 to subsystem blktests-subsystem-1 [5223.088368] nvmet_tcp: enabling port 0 (127.0.0.1:4420) [5223.126086] nvmet: Created discovery controller 1 for subsystem nqn.2014-08.org.nvmexpress.discovery for NQN nqn.2014-08.org.nvmexpress:uuid:0f01fb42-9f7f-4856-b0b3-51e60b8de349. [5223.128453] nvme nvme1: new ctrl: NQN "nqn.2014-08.org.nvmexpress.discovery", addr 127.0.0.1:4420, hostnqn: nqn.2014-08.org.nvmexpress:uuid:0f01fb42-9f7f-4856-b0b3-51e60b8de349 [	2026-06-08	7.5	CVE-2026-46304

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	5233.199447] nvme nvme1: Removing ctrl: NQN "nqn.2014-08.org.nvmexpress.discovery" [5233.227718] ===== [5233.231283] WARNING: possible recursive locking detected [5233.234696] 7.0.0-rc3nvme+ #20 Tainted: G O N [5233.238434] ----- ----- [5233.241852] kworker/u192:6/2413 is trying to acquire lock: [5233.245429] ffff888111632548 ((wq_completion)nvmet-wq){+.+.}-{0:0}, at: touch_wq_lockdep_map+0x26/0x90 [5233.251438] but task is already holding lock: [5233.255254] ffff888111632548 ((wq_completion)nvmet-wq){+.+.}-{0:0}, at: process_one_work+0x5cc/0x6e0 [5233.261125] other info that might help us debug this: [5233.265333] Possible unsafe locking scenario: [5233.269217] CPU0 [5233.270795] ---- [5233.272436] lock((wq_completion)nvmet-wq); [5233.275241] lock((wq_completion)nvmet-wq); [5233.278020] *** DEADLOCK *** [5233.281793] May be due to missing lock nesting notation [5233.286195] 3 locks held by kworker/u192:6/2413: [5233.289192] #0: ffff888111632548 ((wq_completion)nvmet-wq){+.+.}-{0:0}, at: process_one_work+0x5cc/0x6e0 [5233.294569] #1: ffffc9000e2a7e40 ((work_completion)(&queue->release_work)){+.+.}-{0:0}, at: process_one_work+0x1c5/0x6e0 [5233.300128] #2: ffffffff82d7dc40 (rcu_read_lock){....}-{1:3}, at: __flush_work+0x62/0x530 [5233.304290] stack backtrace: [5233.306520] CPU: 4 UID: 0 PID: 2413 Comm: kworker/u192:6 Tainted: G O N 7.0.0-rc3nvme+ #20 PREEMPT(full) [5233.306524] Tainted: [O]=OOT_MODULE, [N]=TEST [5233.306525] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.17.0-0-gb52ca86e094d-prebuilt.qemu.org 04/01/2014 [5233.306527] Workqueue: nvmet-wq nvmet_tcp_release_queue_work [nvmet_tcp] [5233.306532] Call Trace: [5233.306534] <TASK> [5233.306536] dump_stack_lvl+0x73/0xb0 [5233.306552] print_deadlock_bug+0x225/0x2f0 [5233.306556] __lock_acquire+0x13f0/0x2290 [5233.306563] lock_acquire+0xd0/0x300 [5233.306565] ? touch_wq_lockdep_map+0x26/0x90 [5233.306571] ? __flush_work+0x20b/0x530 [5233.306573] ? touch_wq_lockdep_map+0x26/0x90 [5233.306577] touch_wq_lockdep_map+0x3b/0x90 [5233.306580] ? touch_wq_lockdep_map+0x26/0x90 [5233.306584] ? touch_wq_lockdep_map+0x26/0x90 [5233.306588] ? touch_wq_lockdep_map+0x26/0x90 [5233.306592] ? touch_wq_lockdep_map+0x26/0x90 [5233.306596] ? touch_wq_lockdep_map+0x26/0x90 [5233.306600] ? touch_wq_lockdep_map+0x26/0x90 [5233.306604] ? touch_wq_lockdep_map+0x26/0x90 [5233.306608] ? touch_wq_lockdep_map+0x26/0x90 [5233.306612] ? touch_wq_lockdep_map+0x26/0x90 [5233.306616] ? touch_wq_lockdep_map+0x26/0x90 [5233.306620] ? touch_wq_lockdep_map+0x26/0x90 [5233.306624] ? touch_wq_lockdep_map+0x26/0x90 [5233.306628] ? touch_wq_lockdep_map+0x26/0x90 [5233.306632] ? touch_wq_lockdep_map+0x26/0x90 [5233.306636] ? touch_wq_lockdep_map+0x26/0x90 [5233.306640] ? touch_wq_lockdep_map+0x26/0x90 [5233.306644] ? touch_wq_lockdep_map+0x26/0x90 [5233.306648] ? touch_wq_lockdep_map+0x26/0x90 [5233.306652] ? touch_wq_lockdep_map+0x26/0x90 [5233.306656] ? touch_wq_lockdep_map+0x26/0x90 [5233.306660] ? touch_wq_lockdep_map+0x26/0x90 [5233.306664] ? touch_wq_lockdep_map+0x26/0x90 [5233.306668] ? touch_wq_lockdep_map+0x26/0x90 [5233.306672] ? touch_wq_lockdep_map+0x26/0x90 [5233.306676] ? touch_wq_lockdep_map+0x26/0x90 [5233.306680] ? touch_wq_lockdep_map+0x26/0x90 [5233.306684] ? touch_wq_lockdep_map+0x26/0x90 [5233.306688] ? touch_wq_lockdep_map+0x26/0x90 [5233.306692] ? touch_wq_lockdep_map+0x26/0x90 [5233.306696] ? touch_wq_lockdep_map+0x26/0x90 [5233.306700] ? touch_wq_lockdep_map+0x26/0x90 [5233.306704] ? touch_wq_lockdep_map+0x26/0x90 [5233.306708] ? touch_wq_lockdep_map+0x26/0x90 [5233.306712] ? touch_wq_lockdep_map+0x26/0x90 [5233.306716] ? touch_wq_lockdep_map+0x26/0x90 [5233.306720] ? touch_wq_lockdep_map+0x26/0x90 [5233.306724] ? touch_wq_lockdep_map+0x26/0x90 [5233.306728] ? touch_wq_lockdep_map+0x26/0x90 [5233.306732] ? touch_wq_lockdep_map+0x26/0x90 [5233.306736] ? touch_wq_lockdep_map+0x26/0x90 [5233.306740] ? touch_wq_lockdep_map+0x26/0x90 [5233.306744] ? touch_wq_lockdep_map+0x26/0x90 [5233.306748] ? touch_wq_lockdep_map+0x26/0x90 [5233.306752] ? touch_wq_lockdep_map+0x26/0x90 [5233.306756] ? touch_wq_lockdep_map+0x26/0x90 [5233.306760] ? touch_wq_lockdep_map+0x26/0x90 [5233.306764] ? touch_wq_lockdep_map+0x26/0x90 [5233.306768] ? touch_wq_lockdep_map+0x26/0x90 [5233.306772] ? touch_wq_lockdep_map+0x26/0x90 [5233.306776] ? touch_wq_lockdep_map+0x26/0x90 [5233.306780] ? touch_wq_lockdep_map+0x26/0x90 [5233.306784] ? touch_wq_lockdep_map+0x26/0x90 [5233.306788] ? touch_wq_lockdep_map+0x26/0x90 [5233.306792] ? touch_wq_lockdep_map+0x26/0x90 [5233.306796] ? touch_wq_lockdep_map+0x26/0x90 [5233.306800] ? touch_wq_lockdep_map+0x26/0x90 [5233.306804] ? touch_wq_lockdep_map+0x26/0x90 [5233.306808] ? touch_wq_lockdep_map+0x26/0x90 [5233.306812] ? touch_wq_lockdep_map+0x26/0x90 [5233.306816] ? touch_wq_lockdep_map+0x26/0x90 [5233.306820] ? touch_wq_lockdep_map+0x26/0x90 [5233.306824] ? touch_wq_lockdep_map+0x26/0x90 [5233.306828] ? touch_wq_lockdep_map+0x26/0x90 [5233.306832] ? touch_wq_lockdep_map+0x26/0x90 [5233.306836] ? touch_wq_lockdep_map+0x26/0x90 [5233.306840] ? touch_wq_lockdep_map+0x26/0x90 [5233.306844] ? touch_wq_lockdep_map+0x26/0x90 [5233.306848] ? touch_wq_lockdep_map+0x26/0x90 [5233.306852] ? touch_wq_lockdep_map+0x26/0x90 [5233.306856] ? touch_wq_lockdep_map+0x26/0x90 [5233.306860] ? touch_wq_lockdep_map+0x26/0x90 [5233.306864] ? touch_wq_lockdep_map+0x26/0x90 [5233.306868] ? touch_wq_lockdep_map+0x26/0x90 [5233.306872] ? touch_wq_lockdep_map+0x26/0x90 [5233.306876] ? touch_wq_lockdep_map+0x26/0x90 [5233.306880] ? touch_wq_lockdep_map+0x26/0x90 [5233.306884] ? touch_wq_lockdep_map+0x26/0x90 [5233.306888] ? touch_wq_lockdep_map+0x26/0x90 [5233.306892] ? touch_wq_lockdep_map+0x26/0x90 [5233.306896] ? touch_wq_lockdep_map+0x26/0x90 [5233.306900] ? touch_wq_lockdep_map+0x26/0x90 [5233.306904] ? touch_wq_lockdep_map+0x26/0x90 [5233.306908] ? touch_wq_lockdep_map+0x26/0x90 [5233.306912] ? touch_wq_lockdep_map+0x26/0x90 [5233.306916] ? touch_wq_lockdep_map+0x26/0x90 [5233.306920] ? touch_wq_lockdep_map+0x26/0x90 [5233.306924] ? touch_wq_lockdep_map+0x26/0x90 [5233.306928] ? touch_wq_lockdep_map+0x26/0x90 [5233.306932] ? touch_wq_lockdep_map+0x26/0x90 [5233.306936] ? touch_wq_lockdep_map+0x26/0x90 [5233.306940] ? touch_wq_lockdep_map+0x26/0x90 [5233.306944] ? touch_wq_lockdep_map+0x26/0x90 [5233.306948] ? touch_wq_lockdep_map+0x26/0x90 [5233.306952] ? touch_wq_lockdep_map+0x26/0x90 [5233.306956] ? touch_wq_lockdep_map+0x26/0x90 [5233.306960] ? touch_wq_lockdep_map+0x26/0x90 [5233.306964] ? touch_wq_lockdep_map+0x26/0x90 [5233.306968] ? touch_wq_lockdep_map+0x26/0x90 [5233.306972] ? touch_wq_lockdep_map+0x26/0x90 [5233.306976] ? touch_wq_lockdep_map+0x26/0x90 [5233.306980] ? touch_wq_lockdep_map+0x26/0x90 [5233.306984] ? touch_wq_lockdep_map+0x26/0x90 [5233.306988] ? touch_wq_lockdep_map+0x26/0x90 [5233.306992] ? touch_wq_lockdep_map+0x26/0x90 [5233.306996] ? touch_wq_lockdep_map+0x26/0x90 [5233.307000] ? touch_wq_lockdep_map+0x26/0x90 [5233.307004] ? touch_wq_lockdep_map+0x26/0x90 [5233.307008] ? touch_wq_lockdep_map+0x26/0x90 [5233.307012] ? touch_wq_lockdep_map+0x26/0x90 [5233.307016] ? touch_wq_lockdep_map+0x26/0x90 [5233.307020] ? touch_wq_lockdep_map+0x26/0x90 [5233.307024] ? touch_wq_lockdep_map+0x26/0x90 [5233.307028] ? touch_wq_lockdep_map+0x26/0x90 [5233.307032] ? touch_wq_lockdep_map+0x26/0x90 [5233.307036] ? touch_wq_lockdep_map+0x26/0x90 [5233.307040] ? touch_wq_lockdep_map+0x26/0x90 [5233.307044] ? touch_wq_lockdep_map+0x26/0x90 [5233.307048] ? touch_wq_lockdep_map+0x26/0x90 [5233.307052] ? touch_wq_lockdep_map+0x26/0x90 [5233.307056] ? touch_wq_lockdep_map+0x26/0x90 [5233.307060] ? touch_wq_lockdep_map+0x26/0x90 [5233.307064] ? touch_wq_lockdep_map+0x26/0x90 [5233.307068] ? touch_wq_lockdep_map+0x26/0x90 [5233.307072] ? touch_wq_lockdep_map+0x26/0x90 [5233.307076] ? touch_wq_lockdep_map+0x26/0x90 [5233.307080] ? touch_wq_lockdep_map+0x26/0x90 [5233.307084] ? touch_wq_lockdep_map+0x26/0x90 [5233.307088] ? touch_wq_lockdep_map+0x26/0x90 [5233.307092] ? touch_wq_lockdep_map+0x26/0x90 [5233.307096] ? touch_wq_lockdep_map+0x26/0x90 [5233.307100] ? touch_wq_lockdep_map+0x26/0x90 [5233.307104] ? touch_wq_lockdep_map+0x26/0x90 [5233.307108] ? touch_wq_lockdep_map+0x26/0x90 [5233.307112] ? touch_wq_lockdep_map+0x26/0x90 [5233.307116] ? touch_wq_lockdep_map+0x26/0x90 [5233.307120] ? touch_wq_lockdep_map+0x26/0x90 [5233.307124] ? touch_wq_lockdep_map+0x26/0x90 [5233.307128] ? touch_wq_lockdep_map+0x26/0x90 [5233.307132] ? touch_wq_lockdep_map+0x26/0x90 [5233.307136] ? touch_wq_lockdep_map+0x26/0x90 [5233.307140] ? touch_wq_lockdep_map+0x26/0x90 [5233.307144] ? touch_wq_lockdep_map+0x26/0x90 [5233.307148] ? touch_wq_lockdep_map+0x26/0x90 [5233.307152] ? touch_wq_lockdep_map+0x26/0x90 [5233.307156] ? touch_wq_lockdep_map+0x26/0x90 [5233.307160] ? touch_wq_lockdep_map+0x26/0x90 [5233.307164] ? touch_wq_lockdep_map+0x26/0x90 [5233.307168] ? touch_wq_lockdep_map+0x26/0x90 [5233.307172] ? touch_wq_lockdep_map+0x26/0x90 [5233.307176] ? touch_wq_lockdep_map+0x26/0x90 [5233.307180] ? touch_wq_lockdep_map+0x26/0x90 [5233.307184] ? touch_wq_lockdep_map+0x26/0x90 [5233.307188] ? touch_wq_lockdep_map+0x26/0x90 [5233.307192] ? touch_wq_lockdep_map+0x26/0x90 [5233.307196] ? touch_wq_lockdep_map+0x26/0x90 [5233.307200] ? touch_wq_lockdep_map+0x26/0x90 [5233.307204] ? touch_wq_lockdep_map+0x26/0x90 [5233.307208] ? touch_wq_lockdep_map+0x26/0x90 [5233.307212] ? touch_wq_lockdep_map+0x26/0x90 [5233.307216] ? touch_wq_lockdep_map+0x26/0x90 [5233.307220] ? touch_wq_lockdep_map+0x26/0x90 [5233.307224] ? touch_wq_lockdep_map+0x26/0x90 [5233.307228] ? touch_wq_lockdep_map+0x26/0x90 [5233.307232] ? touch_wq_lockdep_map+0x26/0x90 [5233.307236] ? touch_wq_lockdep_map+0x26/0x90 [5233.307240] ? touch_wq_lockdep_map+0x26/0x90 [5233.307244] ? touch_wq_lockdep_map+0x26/0x90 [5233.307248] ? touch_wq_lockdep_map+0x26/0x90 [5233.307252] ? touch_wq_lockdep_map+0x26/0x90 [5233.307256] ? touch_wq_lockdep_map+0x26/0x90 [5233.307260] ? touch_wq_lockdep_map+0x26/0x90 [5233.307264] ? touch_wq_lockdep_map+0x26/0x90 [5233.307268] ? touch_wq_lockdep_map+0x26/0x90 [5233.307272] ? touch_wq_lockdep_map+0x26/0x90 [5233.307276] ? touch_wq_lockdep_map+0x26/0x90 [5233.307280] ? touch_wq_lockdep_map+0x26/0x90 [5233.307284] ? touch_wq_lockdep_map+0x26/0x90 [5233.307288] ? touch_wq_lockdep_map+0x26/0x90 [5233.307292] ? touch_wq_lockdep_map+0x26/0x90 [5233.307296] ? touch_wq_lockdep_map+0x26/0x90 [5233.307300] ? touch_wq_lockdep_map+0x26/0x90 [5233.307304] ? touch_wq_lockdep_map+0x26/0x90 [5233.307308] ? touch_wq_lockdep_map+0x26/0x90 [5233.307312] ? touch_wq_lockdep_map+0x26/0x90 [5233.307316] ? touch_wq_lockdep_map+0x26/0x90 [5233.307320] ? touch_wq_lockdep_map+0x26/0x90 [5233.307324] ? touch_wq_lockdep_map+0x26/0x90 [5233.307328] ? touch_wq_lockdep_map+0x26/0x90 [5233.307332] ? touch_wq_lockdep_map+0x26/0x90 [5233.307336] ? touch_wq_lockdep_map+0x26/0x90 [5233.307340] ? touch_wq_lockdep_map+0x26/0x90 [5233.307344] ? touch_wq_lockdep_map+0x26/0x90 [5233.307348] ? touch_wq_lockdep_map+0x26/0x90 [5233.307352] ? touch_wq_lockdep_map+0x26/0x90 [5233.307356] ? touch_wq_lockdep_map+0x26/0x90 [5233.307360] ? touch_wq_lockdep_map+0x26/0x90 [5233.307364] ? touch_wq_lockdep_map+0x26/0x90 [5233.307368] ? touch_wq_lockdep_map+0x26/0x90 [5233.307372] ? touch_wq_lockdep_map+0x26/0x90 [5233.307376] ? touch_wq_lockdep_map+0x26/0x90 [5233.307380] ? touch_wq_lockdep_map+0x26/0x90 [5233.307384] ? touch_wq_lockdep_map+0x26/0x90 [5233.307388] ? touch_wq_lockdep_map+0x26/0x90 [5233.307392] ? touch_wq_lockdep_map+0x26/0x90 [5233.307396] ? touch_wq_lockdep_map+0x26/0x90 [5233.307400] ? touch_wq_lockdep_map+0x26/0x90 [5233.307404] ? touch_wq_lockdep_map+0x26/0x90 [5233.307408] ? touch_wq_lockdep_map+0x26/0x90 [5233.307412] ? touch_wq_lockdep_map+0x26/0x90 [5233.307416] ? touch_wq_lockdep_map+0x26/0x90 [5233.307420] ? touch_wq_lockdep_map+0x26/0x90 [5233.307424] ? touch_wq_lockdep_map+0x26/0x90 [5233.307428] ? touch_wq_lockdep_map+0x26/0x90 [5233.307432] ? touch_wq_lockdep_map+0x26/0x90 [5233.307436] ? touch_wq_lockdep_map+0x26/0x90 [5233.307440] ? touch_wq_lockdep_map+0x26/0x90 [5233.307444] ? touch_wq_lockdep_map+0x26/0x90 [5233.307448] ? touch_wq_lockdep_map+0x26/0x90 [5233.307452] ? touch_wq_lockdep_map+0x26/0x90 [5233.307456] ? touch_wq_lockdep_map+0x26/0x90 [5233.307460] ? touch_wq_lockdep_map+0x26/0x90 [5233.307464] ? touch_wq_lockdep_map+0x26/0x90 [5233.307468] ? touch_wq_lockdep_map+0x26/0x90 [5233.307472] ? touch_wq_lockdep_map+0x26/0x90 [5233.307476] ? touch_wq_lockdep_map+0x26/0x90 [5233.307480] ? touch_wq_lockdep_map+0x26/0x90 [5233.307484] ? touch_wq_lockdep_map+0x26/0x90 [5233.307488] ? touch_wq_lockdep_map+0x26/0x90 [5233.307492] ? touch_wq_lockdep_map+0x26/0x90 [5233.307496] ? touch_wq_lockdep_map+0x26/0x90 [5233.307500] ? touch_wq_lockdep_map+0x26/0x90 [5233.307504] ? touch_wq_lockdep_map+0x26/0x90 [5233.307508] ? touch_wq_lockdep_map+0x26/0x90 [5233.307512] ? touch_wq_lockdep_map+0x26/0x90 [5233.307516] ? touch_wq_lockdep_map+0x26/0x90 [5233.307520] ? touch_wq_lockdep_map+0x26/0x90 [5233.307524] ? touch_wq_lockdep_map+0x26/0x90 [5233.307528] ? touch_wq_lockdep_map+0x26/0x90 [5233.307532] ? touch_wq_lockdep_map+0x26/0x90 [5233.307536] ? touch_wq_lockdep_map+0x26/0x90 [5233.307540] ? touch_wq_lockdep_map+0x26/0x90 [5233.307544] ? touch_wq_lockdep_map+0x26/0x90 [5233.307548] ? touch_wq_lockdep_map+0x26/0x90 [5233.307552] ? touch_wq_lockdep_map+0x26/0x90 [5233.307556] ? touch_wq_lockdep_map+0x26/0x90 [5233.307560] ? touch_wq_lockdep_map+0x26/0x90 [5233.307564] ? touch_wq_lockdep_map+0x26/0x90 [5233.307568] ? touch_wq_lockdep_map+0x26/0x90 [5233.307572] ? touch_wq_lockdep_map+0x26/0x90 [5233.307576] ? touch_wq_lockdep_map+0x26/0x90 [5233.307580] ? touch_wq_lockdep_map+0x26/0x90 [5233.307584] ? touch_wq_lockdep_map+0x26/0x90 [5233.307588] ? touch_wq_lockdep_map+0x26/0x90 [5233.307592] ? touch_wq_lockdep_map+0x26/0x90 [5233.307596] ? touch_wq_lockdep_map+0x26/0x90 [5233.307600] ? touch_wq_lockdep_map+0x26/0x90 [5233.307604] ? touch_wq_lockdep_map+0x26/0x90 [5233.307608] ? touch_wq_lockdep_map+0x26/0x90 [5233.307612] ? touch_wq_lockdep_map+0x26/0x90 [5233.307616] ? touch_wq_lockdep_map+0x26/0x90 [5233.307620] ? touch_wq_lockdep_map+0x26/0x90 [5233.307624] ? touch_wq_lockdep_map+0x26/0x90 [5233.307628] ? touch_wq_lockdep_map+0x26/0x90 [5233.307632] ? touch_wq_lockdep_map+0x26/0x90 [5233.307636] ? touch_wq_lockdep_map+0x26/0x90 [5233.307640] ? touch_wq_lockdep_map+0x26/0x90 [5233.307644] ? touch_wq_lockdep_map+0x26/0x90 [5233.307648] ? touch_wq_lockdep_map+0x26/0x90 [5233.307652] ? touch_wq_lockdep_map+0x26/0x90 [5233.307656] ? touch_wq_lockdep_map+0x26/0x90 [5233.307660] ? touch_wq_lockdep_map+0x26/0x90 [5233.307664] ? touch_wq_lockdep_map+0x26/0x90 [5233.307668] ? touch_wq_lockdep_map+0x26/0x90 [5233.307672] ? touch_wq_lockdep_map+0x26/0x90 [5233.307676] ? touch_wq_lockdep_map+0x26/0x90 [5233.307680] ? touch_wq_lockdep_map+0x26/0x90 [5233.307684] ? touch_wq_lockdep_map+0x26/0x90 [5233.307688] ? touch_wq_lockdep_map+0x26/0x90 [5233.307692] ? touch_wq_lockdep_map+0x26/0x90 [5233.307696] ? touch_wq_lockdep_map+0x26/0x90 [5233.307700] ? touch_wq_lockdep_map+0x26/0x90 [5233.307704] ? touch_wq_lockdep_map+0x26/0x90 [5233.307708] ? touch_wq_lockdep_map+0x26/0x90 [5233.307712] ? touch_wq_lockdep_map+0x26/0x90 [5233.307716] ? touch_wq_lockdep_map+0x26/0x90 [5233.307720] ? touch_wq_lockdep_map+0x26/0x90 [5233.307724] ? touch_wq_lockdep_map+0x26/0x90 [5233.307728] ? touch_wq_lockdep_map+0x26/0x90 [5233.307732] ? touch_wq_lockdep_map+0x26/0x90 [5233.307736] ? touch_wq_lockdep_map+0x26/0x90 [5233.307740] ? touch_wq_lockdep_map+0x26/0x90 [5233.307744] ? touch_wq_lockdep_map+0x26/0x90 [5233.307748] ? touch_wq_lockdep_map+0x26/0x90 [5233.307752] ? touch_wq_lockdep_map+0x26/0x90 [5233.307756] ? touch_wq_lockdep_map+0x26/0x90 [5233.307760] ? touch_wq_lockdep_map+0x26/0x90 [5233.307764] ? touch_wq_lockdep_map+0x26/0x90 [5233.307768] ? touch_wq_lockdep_map+0x26/0x90 [5233.307772] ? touch_wq_lockdep_map+0x26/0x90 [5233.307776] ? touch_wq_lockdep_map+0x26/0x90 [5233.307780] ? touch_wq_lockdep_map+0x26/0x90 [5233.307784] ? touch_wq_lockdep_map+0x26/0x90 [5233.307788] ? touch_wq_lockdep_map+0x26/0x90 [5233.307792] ? touch_wq_lockdep_map+0x26/0x90 [5233.307796] ? touch_wq_lockdep_map+0x26/0x90 [5233.307800] ? touch_wq_lockdep_map+0x26/0x90 [5233.307804] ? touch_wq_lockdep_map+0x26/0x90 [5233.307808] ? touch_wq_lockdep_map+0x26/0x90 [5233.307812] ? touch_wq_lockdep_map+0x26/0x90 [5233.307816] ? touch_wq_lockdep_map+0x26/0x90 [5233.307820] ? touch_wq_lockdep_map+0x26/0x90 [5233.307824] ? touch_wq_lockdep_map+0x26/0x90 [5233.307828] ? touch_wq_lockdep_map+0x26/0x90 [5233.307832] ? touch_wq_lockdep_map+0x26/0x90 [5233.307836] ? touch_wq_lockdep_map+0x26/0x90 [5233.307840] ? touch_wq_lockdep_map+0x26/0x90 [5233.307844] ? touch_wq_lockdep_map+0x26/0x90 [5233.307848] ? touch_wq_lockdep_map+0x26/0x90 [5233.307852] ? touch_wq_lockdep_map+0x26/0x90 [5233.307856] ? touch_wq_lockdep_map+0x26/0x90 [5233.307860] ? touch_wq_lockdep_map+0x26/0x90 [5233.307864] ? touch_wq_lockdep_map+0x26/0x90 [5233.307868] ? touch_wq_lockdep_map+0x26/0x90 [5233.307872] ? touch_wq_lockdep_map+0x26/0x90 [5233.307876] ? touch_wq_lockdep_map+0x26/0x90 [5233.307880] ? touch_wq_lockdep_map+0x26/0x90 [5233.307884] ? touch_wq_lockdep_map+0x26/0x90 [5233.307888] ? touch_wq_lockdep_map+0x26/0x90 [5233.307892] ? touch_wq_lockdep_map+0x26/0x90 [5233.307896] ? touch_wq_lockdep_map+0x26/0x90 [5233.307900] ? touch_wq_lockdep_map+0x26/0x90 [5233.307904] ? touch_wq_lockdep_map+0x26/0x90 [5233.307908] ? touch_wq_lockdep_map+0x26/0x90 [5233.307912] ? touch_wq_lockdep_map+0x26/0x90 [5233.307916] ? touch_wq_lockdep_map+0x26/0x90 [5233.307920] ? touch_wq_lockdep_map+0x26/0x90 [5233.307924] ? touch_wq_lockdep_map+0x26/0x90 [5233.307928] ? touch_wq_lockdep_map+0x26/0x90 [5233.307932] ? touch_wq_lockdep_map+0x26/0x90 [5233.307936] ? touch_wq_lockdep_map+0x26/0x90 [5233.307940] ? touch_wq_lockdep_map+0x26/0x90 [5233.307944] ? touch_wq_lockdep_map+0x26/0x90 [5233.307948] ? touch_wq_lockdep_map+0x26/0x90 [5233.307952] ? touch_wq_lockdep_map+0x26/0x90 [5233.307956] ? touch_wq_lockdep_map+0x26/0x90 [5233.307960] ? touch_wq_lockdep_map+0x26/0x90 [5233.307964] ? touch_wq_lockdep_map+0x26/0x90 [5233.307968] ? touch_wq_lockdep_map+0x26/0x90 [5233.307972] ? touch_wq_lockdep_map+0x26/0x90 [5233.307976] ? touch_wq_lockdep_map+0x26/0x90 [5233.307980] ? touch_wq_lockdep_map+0x26/0x90 [5233.307984] ? touch_wq_lockdep_map+0x26/0x90 [5233.307988] ? touch_wq_lockdep_map+0x26/0x90 [5233.307992] ? touch_wq_lockdep_map+0x26/0x90 [5233.307996] ? touch_wq_lockdep_map+0x26/0x90 [5233.308000] ? touch_wq_lockdep_map+0x26/0x90 [5233.308004] ? touch_wq_lockdep_map+0x26/0x90 [5233.308008] ? touch_wq_lockdep_map+0x26/0x90 [			

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	[<805fca70>] netif_receive_skb_list_internal+0x324/0x364 [<805fd120>] napi_complete_done+0x68/0x2a4 [<8058de5c>] mtk_napi_rx+0x228/0xfec [<805fd398>] __napi_poll+0x3c/0x1c4 [<805fd754>] napi_threaded_poll_loop+0x234/0x29c [<805fd848>] napi_threaded_poll+0x8c/0xb0 [<80053544>] kthread+0x104/0x12c [<80002bd8>] ret_from_kernel_thread+0x14/0x1c Code: 02d51821 1060045b 00000000 <8c640000> 3084000f 2c820005 144001a2 00042080 8e220000 To reduce the attack surface and maintain performance, do not process PPPoE PFC frames. [1] https://lore.kernel.org/r/20220630231016.GA392@debian.home			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/userq: fix access to stale wptr mapping Use drm_exec to take both locks i.e vm root bo and wptr_obj bo to access the mapping data properly. This fixes the security issue of unmap the wptr_obj while a queue creation is in progress and passing other bo at same address. (cherry picked from commit 1fc6c8ab45dbee096469c08c13f6099d57a52d6c)	2026-06-08	7.8	CVE-2026-46311
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_ct: Only release RCU read lock after ct_ft When looking up a flow table in act_ct in tcf_ct_flow_table_get(), rhashtable_lookup_fast() internally opens and closes an RCU read critical section before returning ct_ft. The tcf_ct_flow_table_cleanup_work() can complete before refcount_inc_not_zero() is invoked on the returned ct_ft resulting in a UAF on the already freed ct_ft object. This vulnerability can lead to privilege escalation. Analysis from zdi-disclosures@trendmicro.com: When initializing act_ct, tcf_ct_init() is called, which internally triggers tcf_ct_flow_table_get(). static int tcf_ct_flow_table_get(struct net *net, struct tcf_ct_params *params) { struct zones_ht_key key = { .net = net, .zone = params->zone }; struct tcf_ct_flow_table *ct_ft; int err = -ENOMEM; mutex_lock(&zones_mutex); ct_ft = rhashtable_lookup_fast(&zones_ht, &key, zones_params); // [1] if (ct_ft && refcount_inc_not_zero(&ct_ft->ref)) // [2] goto out_unlock; ... } static __always_inline void *rhashtable_lookup_fast(struct rhashtable *ht, const void *key, const struct rhashtable_params params) { void *obj; rcu_read_lock(); obj = rhashtable_lookup(ht, key, params); rcu_read_unlock(); return obj; } At [1], rhashtable_lookup_fast() looks up and returns the corresponding ct_ft from zones_ht . The lookup is performed within an RCU read critical section through rcu_read_lock() / rcu_read_unlock(), which prevents the object from being freed. However, at the point of function return, rcu_read_unlock() has already been called, and there is nothing preventing ct_ft from being freed before reaching refcount_inc_not_zero(&ct_ft->ref) at [2]. This interval becomes the race window, during which ct_ft can be freed. Free Process: tcf_ct_flow_table_put() is executed through the path tcf_ct_cleanup() call_rcu() tcf_ct_params_free_rcu() tcf_ct_params_free() tcf_ct_flow_table_put(). static void tcf_ct_flow_table_put(struct tcf_ct_flow_table *ct_ft) { if (refcount_dec_and_test(&ct_ft->ref)) { rhashtable_remove_fast(&zones_ht, &ct_ft->node, zones_params); INIT_RCU_WORK(&ct_ft->rwork, tcf_ct_flow_table_cleanup_work); // [3] queue_rcu_work(act_ct_wq, &ct_ft->rwork); } } At [3], tcf_ct_flow_table_cleanup_work() is scheduled as RCU work static void tcf_ct_flow_table_cleanup_work(struct work_struct *work) { struct tcf_ct_flow_table *ct_ft; struct flow_block *block; ct_ft = container_of(to_rcu_work(work), struct tcf_ct_flow_table, rwork); nf_flow_table_free(&ct_ft->nf_ft); block = &ct_ft->nf_ft.flow_block; down_write(&ct_ft->nf_ft.flow_block_lock); WARN_ON(!list_empty(&block->cb_list)); up_write(&ct_ft->nf_ft.flow_block_lock); kfree(ct_ft); // [4] module_put(THIS_MODULE); } tcf_ct_flow_table_cleanup_work() frees ct_ft at [4]. When this function executes between [1] and [2], UAF occurs. This race condition has a very	2026-06-09	7.8	CVE-2026-46319

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	short race window, making it generally difficult to trigger. Therefore, to trigger the vulnerability an msleep(100) was inserted after[1]			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tap: free page on error paths in tap_get_user_xdp() tap_get_user_xdp() rejects a frame shorter than ETH_HLEN with -EINVAL, and returns -ENOMEM when build_skb() fails. Both paths jump to the err label without freeing the page that vhost_net_build_xdp() allocated for the frame. tap_sendmsg() discards the per-buffer return value and always returns 0, so vhost_tx_batch() takes the success path and never frees the page; each rejected frame in a batch leaks one page-frag chunk. Free the page on both error paths, before the skb is built. This is the tap counterpart of the same leak in tun_xdp_one().	2026-06-09	7.4	CVE-2026-46320
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tun: free page on short-frame rejection in tun_xdp_one() tun_xdp_one() returns -EINVAL on a frame shorter than ETH_HLEN without freeing the page that vhost_net_build_xdp() allocated for it. tun_sendmsg() discards that -EINVAL and still returns total_len, so vhost_tx_batch() takes the success path and never frees the page; each short frame in a batch leaks one page-frag chunk. A local process that can open /dev/net/tun and /dev/vhost-net can hit this path: it attaches a tun/tap device as the vhost-net backend and feeds TX descriptors whose length minus the virtio-net header is below ETH_HLEN. Each kick leaks the page-frag chunks for that batch, and a tight submission loop exhausts host memory and triggers an OOM panic. Free the page before returning -EINVAL, matching the XDP-program error path in the same function.	2026-06-09	7.1	CVE-2026-46321
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tun: free page on build_skb failure in tun_xdp_one() When build_skb() fails in tun_xdp_one(), the function sets ret to -ENOMEM and jumps to the out label, which returns without freeing the page that vhost_net_build_xdp() allocated for the frame. As with the short-frame rejection path, tun_sendmsg() discards the per-buffer error and still returns total_len, so vhost_tx_batch() takes the success path and never frees the page. Each build_skb() failure in a batch leaks one page-frag chunk. Free the page before taking the error path, matching the put_page() the other error exits of tun_xdp_one() already perform.	2026-06-09	7.1	CVE-2026-46322
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: gro: don't merge zcopy skbs skb_gro_receive() can currently copy frags between the source and GRO skb, without checking the zerocopy status, and in particular the SKBFL_MANAGED_FRAG_REFS flag. When SKBFL_MANAGED_FRAG_REFS is set, the skb doesn't hold a reference on the pages in shinfo->frags. Appending those frags to another skb's frags without fixing up the page refcount can lead to UAF. When either the last skb in the GRO chain (the one we would append frags to) or the source skb is zerocopy, don't merge the skbs.	2026-06-09	7.8	CVE-2026-46323
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: use list_del_rcu for netlink hooks nft_netdev_unregister_hooks and __nft_unregister_flowtable_net_hooks need to use list_del_rcu(), this list can be walked by concurrent dumpers. Add a new helper and use it consistently.	2026-06-09	7.8	CVE-2026-46324
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dm: fix unlocked test for dm_suspended_md The function dm_blk_report_zones tests if the device is suspended with the "dm_suspended_md" call. However, this function is called without holding any locks, so the device may be suspended just after it. Move the call to dm_suspended_md after dm_get_live_table, so that the device can't be suspended after the suspended state was tested.	2026-06-09	7.8	CVE-2026-46327
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix rlimit for posix cpu timers Posix cpu timers requires an additional step beyond setting the rlimit. Refactor the code so its clear	2026-06-09	7.3	CVE-2026-46328

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	when what code is setting the limit and conditionally update the posix cpu timers when appropriate.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Revert "net/smc: Introduce TCP ULP support" This reverts commit d7cd421da9da2cc7b4d25b8537f66db5c8331c40. As reported by Al Viro, the TCP ULP support for SMC is fundamentally broken. The implementation attempts to convert an active TCP socket into an SMC socket by modifying the underlying `struct file`, dentry, and inode in-place, which violates core VFS invariants that assume these structures are immutable for an open file, creating a risk of use after free errors and general system instability. Given the severity of this design flaw and the fact that cleaner alternatives (e.g., LD_PRELOAD, BPF) exist for legacy application transparency, the correct course of action is to remove this feature entirely.	2026-06-09	7.8	CVE-2026-46330
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: 9p: fix access mode flags being ORed instead of replaced Since commit 1f3e4142c0eb ("9p: convert to the new mount API"), v9fs_apply_options() applies parsed mount flags with = onto flags already set by v9fs_session_init(). For 9P2000.L, session_init sets V9FS_ACCESS_CLIENT as the default, so when the user mounts with "access=user", both bits end up set. Access mode checks compare against exact values, so having both bits set matches neither mode. This causes v9fs_fid_lookup() to fall through to the default switch case, using INVALID_UID (nobody/65534) instead of current_fsuid() for all fid lookups. Root is then unable to chown or perform other privileged operations. Fix by clearing the access mask before applying the user's choice.	2026-06-09	7.7	CVE-2026-52906
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: media: rockchip: rkcf: fix off by one bugs Change these comparisons from > vs >= to avoid accessing one element beyond the end of the arrays. While at it, use ARRAY_SIZE instead of the _MAX enum values. [fix cosmetic issues]	2026-06-09	7.8	CVE-2026-52907
LiteSpeed Technologies--cPanel Plugin	LiteSpeed cPanel plugin before 2.4.8 (as distributed in LiteSpeed WHM PlugIn before 5.3.2.0) mishandles symlinks provided by a user with FTP or web shell access on a shared hosting server running CloudLinux/CageFS, as exploited in the wild in May 2026.	2026-06-14	8.5	CVE-2026-54420
MacWarrior--clipbucket-v5	ClipBucket v5 is an open source video sharing platform. Prior to version 5.5.3 - #140, ClipBucket's Remote Play feature allows any authenticated user to add a video by importing an external URL as the source. Some shell commands are run with the URL as a parameter. The URL is concatenated directly into shell commands without escaping then executed, so any shell metacharacter in the URL is interpreted. This results in arbitrary command execution. This issue has been patched in version 5.5.3 - #140.	2026-06-11	9.8	CVE-2026-42846
MacWarrior--clipbucket-v5	ClipBucket v5 is an open source video sharing platform. Prior to version 5.5.3 - #129, the actions/progress_video.php endpoint is vulnerable to blind SQL injection. Any unauthenticated user can exploit the ids parameter to execute SQL queries and exfiltrate sensitive data. This issue has been patched in version 5.5.3 - #129.	2026-06-11	9.8	CVE-2026-45060
MacWarrior--clipbucket-v5	ClipBucket v5 is an open source video sharing platform. Prior to version 5.5.3 - #132, any authenticated user who can upload videos can add multiple subtitles from different files and change their title (English, Spanish...). The POST /actions/subtitle_edit.php request used to change their title includes a number parameter which is vulnerable to SQL Injection. A boolean-based blind SQL injection can be used to exfiltrate sensitive data. This issue has been patched in version 5.5.3 - #132.	2026-06-11	8.8	CVE-2026-45418
makeplane--plane	Plane is an open-source project management tool. Prior to version 1.3.1, there is a cross-workspace asset authorization bypass lets any authenticated user read, copy, delete, and overwrite assets in other Plane workspaces. This issue has been patched in version 1.3.1.	2026-06-10	8.3	CVE-2026-46558
MariaDB--server	MariaDB server is a community developed fork of MySQL server. Versions 10.6.1 through 10.6.26, 10.11.1 through 10.11.17, 11.4.1 through 11.4.11,	2026-06-11	10	CVE-2026-49261

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	11.8.1 through 11.8.7, and 12.3.1 with `wsrep_notify_cmd` enabled would execute shell commands embedded in the name of the joiner node. This is fixed in 10.6.27, 10.11.18, 11.4.12, 11.8.8, and 12.3.2. As a workaround, anyone who cannot upgrade now should disable `wsrep_notify_cmd`.			
MariaDB--server	MariaDB server is a community developed fork of MySQL server. From versions 10.6.1 to before 10.6.26, 10.11.1 to before 10.11.17, 11.4.1 to before 11.4.11, 11.8.1 to before 11.8.7, and 12.3.1, during the SST the donor node is interpolating parameters that the joiner sent into the command line. Not all parameters were properly validated which could allow a malicious joiner to execute arbitrary shell commands on the donor side via the mariabackup SST method. This issue has been patched in versions 10.6.26, 10.11.17, 11.4.11, 11.8.7, and 12.3.2.	2026-06-12	8	CVE-2026-44168
MariaDB--server	MariaDB server is a community developed fork of MySQL server. From versions 10.6.1 to before 10.6.27, 10.11.1 to before 10.11.18, 11.4.1 to before 11.4.12, 11.8.1 to before 11.8.8, and 12.3.1, during the SST the donor node is interpolating parameters that the joiner sent into the command line. Not all parameters were properly validated which could allow a malicious joiner to execute arbitrary shell commands on the donor side via the rsync SST method. This issue has been patched in versions 10.6.27, 10.11.18, 11.4.12, 11.8.8, and 12.3.2.	2026-06-12	8	CVE-2026-48163
MariaDB--server	MariaDB server is a community developed fork of MySQL server. From versions 10.6.1 to before 10.6.27, 10.11.1 to before 10.11.18, 11.4.1 to before 11.4.12, 11.8.1 to before 11.8.8, and 12.3.1, a high-privileged MariaDB user could've used wsrep_sst_receive_address or wsrep_sst_donor global system variables to execute shell commands as the uid of the mariadb process on the galera joiner node. This issue has been patched in versions 10.6.27, 10.11.18, 11.4.12, 11.8.8, and 12.3.2.	2026-06-12	8	CVE-2026-48165
Mattermost--Mattermost	Mattermost versions 11.6.x <= 11.6.1, 11.5.x <= 11.5.4, 10.11.x <= 10.11.15, 10.11.x <= 10.11.16 Mattermost fails to require role-management authorization when setting the scheme_admin flag on group syncable link and patch endpoints, which allows a user with group-link permissions to escalate themselves and group members to team or channel admin via crafted API requests.. Mattermost Advisory ID: MMSA-2026-00665	2026-06-12	8.8	CVE-2026-7387
Mattermost--Mattermost	Mattermost versions 11.6.x <= 11.6.1, 11.5.x <= 11.5.4, 10.11.x <= 10.11.15, 10.11.x <= 10.11.16 Mattermost fails to sanitize FileInfo.Name received from federated peers during shared channel file sync, which allows an attacker who controls a federated server to write files to arbitrary locations within the target server's filestore via path traversal sequences in the filename field.. Mattermost Advisory ID: MMSA-2026-00661	2026-06-12	7.6	CVE-2026-6961
Md. Shamim Shahnewaz--Single Personal Message	Single Personal Message 1.0.3 contains an SQL injection vulnerability that allows authenticated users to execute arbitrary SQL queries by injecting malicious code through the message parameter. Attackers can access the admin interface and supply crafted SQL statements in the message parameter to extract sensitive database information including user credentials and site configuration data.	2026-06-09	7.1	CVE-2016-20063
mem0ai--mem0	Mem0 versions through 0.2.8, fixed in commit ae7f406, contain a missing authorization vulnerability in the self-hosted server component where the POST /configure endpoint modifies global LLM provider and embedder configuration but only verifies authentication via JWT or X-API-Key without validating the caller's role. Any authenticated user holding a distributed API key can redirect all LLM and embedder traffic to an attacker-controlled server, with the malicious configuration persisted to PostgreSQL and surviving server restarts to affect all users and API keys on the instance.	2026-06-09	8.1	CVE-2026-49948
Microsoft--.NET 10.0	Improper authorization in .NET allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-45490
Microsoft--.NET 10.0	Uncontrolled resource consumption in ASP.NET Core allows an unauthorized attacker to deny service over a network.	2026-06-09	7.5	CVE-2026-45591

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Azure Kubernetes Service	Improper limitation of a pathname to a restricted directory ('path traversal') in Microsoft Azure Kubernetes Service allows an authorized attacker to execute code locally.	2026-06-09	8.8	CVE-2026-32193
Microsoft--Azure Stack Edge	External control of file name or path in Azure Stack Edge allows an unauthorized attacker to execute code over a network.	2026-06-09	9.8	CVE-2026-47643
Microsoft--Azure Stack Edge	Improper neutralization of input during web page generation ('cross-site scripting') in Azure Stack Edge allows an authorized attacker to perform spoofing over a network.	2026-06-09	8.4	CVE-2026-41098
Microsoft--Linux kernel - Microsoft MANA Network Driver	Use after free in Linux MANA Driver allows an authorized attacker to elevate privileges locally.	2026-06-09	8.2	CVE-2026-45476
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information over a network.	2026-06-09	8.2	CVE-2026-44822
Microsoft--Microsoft 365 Apps for Enterprise	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	8.4	CVE-2026-45456
Microsoft--Microsoft 365 Apps for Enterprise	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	8.4	CVE-2026-45458
Microsoft--Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	8.4	CVE-2026-45461
Microsoft--Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	8.4	CVE-2026-45463
Microsoft--Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	8.4	CVE-2026-45472
Microsoft--Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	8.4	CVE-2026-45474
Microsoft--Microsoft 365 Apps for Enterprise	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-44817
Microsoft--Microsoft 365 Apps for Enterprise	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-06-09	7	CVE-2026-44818
Microsoft--Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-44819
Microsoft--Microsoft 365 Apps for Enterprise	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-44820
Microsoft--Microsoft 365	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-44823

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Apps for Enterprise				
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-44824
Microsoft-- Microsoft 365 Apps for Enterprise	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-45457
Microsoft-- Microsoft 365 Apps for Enterprise	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-45469
Microsoft-- Microsoft 365 Apps for Enterprise	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-45471
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-45475
Microsoft-- Microsoft 365 Apps for Enterprise	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-45486
Microsoft-- Microsoft 365 Apps for Enterprise	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-45643
Microsoft-- Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-45645
Microsoft-- Microsoft 365 Apps for Enterprise	Use after free in Microsoft Office Click-To-Run allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-47293
Microsoft-- Microsoft Dynamics 365 (on-premises) version 9.1	Improper handling of insufficient permissions or privileges in Microsoft Dynamics 365 (on-premises) allows an authorized attacker to elevate privileges over a network.	2026-06-09	8.8	CVE-2026-40371
Microsoft-- Microsoft Excel for Android	Integer overflow or wraparound in Windows Win32K - GRFX allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-44803
Microsoft-- Microsoft Excel for Android	Integer overflow or wraparound in Windows Win32K - GRFX allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-44812
Microsoft-- Microsoft Excel for Android	Improper access control in Office for Android allows an unauthorized attacker to perform spoofing locally.	2026-06-09	7.1	CVE-2026-45649
Microsoft-- Microsoft Exchange Server 2016 Cumulative Update 23	Server-side request forgery (ssrf) in Microsoft Exchange Server allows an authorized attacker to disclose information over a network.	2026-06-09	8.1	CVE-2026-45503

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft-- Microsoft Exchange Server 2016 Cumulative Update 23	Server-side request forgery (ssrf) in Microsoft Exchange Server allows an authorized attacker to elevate privileges over a network.	2026-06-09	8.8	CVE-2026-45504
Microsoft-- Microsoft Exchange Server 2016 Cumulative Update 23	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	2026-06-09	8.1	CVE-2026-47631
Microsoft-- Microsoft Exchange Server 2016 Cumulative Update 23	Improper control of generation of code ('code injection') in Microsoft Exchange Server allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5	CVE-2026-45583
Microsoft-- Microsoft Live Share Canvas SDK	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Live Share Canvas SDK allows an authorized attacker to elevate privileges over a network.	2026-06-09	8	CVE-2026-45644
Microsoft-- Microsoft Office LTSC 2024	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	8.4	CVE-2026-47635
Microsoft-- Microsoft PC Manager	Improper access control in Microsoft PC Manager allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.8	CVE-2026-49161
Microsoft-- Microsoft PC Manager	Improper link resolution before file access ('link following') in Microsoft PC Manager allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-50511
Microsoft-- Microsoft PC Manager	Improper link resolution before file access ('link following') in Microsoft PC Manager allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-50512
Microsoft-- Microsoft PowerToys	Improper authorization in Microsoft PowerToys allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-42902
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to elevate privileges over a network.	2026-06-09	8.8	CVE-2026-45484
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper authorization in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-06-09	8	CVE-2026-47298
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	7.3	CVE-2026-45481
Microsoft-- Microsoft SharePoint Server 2019	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	7.3	CVE-2026-47634
Microsoft-- Microsoft Teams for Android	Improper neutralization of special elements in output used by a downstream component ('injection') in Microsoft Teams for Android allows an authorized attacker to disclose information over a network.	2026-06-09	8.1	CVE-2026-42835

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft-- Microsoft Visual Studio Code CoPilot Chat Extension	Improper limitation of a pathname to a restricted directory ('path traversal') in GitHub Copilot and Visual Studio Code allows an unauthorized attacker to bypass a security feature locally.	2026-06-09	8.4	CVE-2026-45482
Microsoft-- Nuance PowerScribe 360 4.0	Deserialization of untrusted data in Nuance PowerScribe allows an unauthorized attacker to execute code over a network.	2026-06-09	9.8	CVE-2026-26142
Microsoft-- Remote Desktop client for Windows Desktop	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	8.8	CVE-2026-42985
Microsoft-- Remote Desktop client for Windows Desktop	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5	CVE-2026-42909
Microsoft-- Remote Desktop client for Windows Desktop	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5	CVE-2026-42913
Microsoft-- Remote Desktop client for Windows Desktop	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5	CVE-2026-44799
Microsoft-- Remote Desktop client for Windows Desktop	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5	CVE-2026-44801
Microsoft-- Remote Desktop client for Windows Desktop	Out-of-bounds read in Windows RDP allows an unauthorized attacker to disclose information over a network.	2026-06-09	7.5	CVE-2026-45639
Microsoft--Visual Studio Code	Improper input validation in Visual Studio Code allows an unauthorized attacker to elevate privileges over a network.	2026-06-09	9.6	CVE-2026-47281
Microsoft--Visual Studio Code	Improper input validation in Visual Studio Code allows an unauthorized attacker to elevate privileges over a network.	2026-06-09	7.5	CVE-2026-40376
Microsoft--Visual Studio Code	Improper input validation in Visual Studio Code allows an unauthorized attacker to bypass a security feature locally.	2026-06-09	7.1	CVE-2026-48569
Microsoft--Visual Studio Code - MSSQL Extension	Inclusion of functionality from untrusted control sphere in Visual Studio Code allows an unauthorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-47292
Microsoft-- Windows 10 Version 1607	Stack-based buffer overflow in Windows DHCP Client allows an unauthorized attacker to execute code over a network.	2026-06-09	9.8	CVE-2026-44815
Microsoft-- Windows 10 Version 1607	No cwe for this issue in Windows DHCP Server allows an unauthorized attacker to perform tampering over a network.	2026-06-09	9.1	CVE-2026-45602
Microsoft-- Windows 10 Version 1607	Integer overflow or wraparound in Windows HTTP.sys allows an unauthorized attacker to execute code over a network.	2026-06-09	9.8	CVE-2026-47291

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1607	Use after free in Universal Plug and Play (upnp.dll) allows an unauthorized attacker to execute code over a network.	2026-06-09	8.1	CVE-2026-45599
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows Hyper-V allows an unauthorized attacker to execute code locally.	2026-06-09	8.4	CVE-2026-45607
Microsoft--Windows 10 Version 1607	Use after free in Universal Plug and Play (upnp.dll) allows an unauthorized attacker to execute code over a network.	2026-06-09	8.1	CVE-2026-45635
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	8.8	CVE-2026-47289
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	8.8	CVE-2026-47653
Microsoft--Windows 10 Version 1607	Trust boundary violation in Windows Attestation allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-33828
Microsoft--Windows 10 Version 1607	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-34335
Microsoft--Windows 10 Version 1607	Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability	2026-06-09	7.8	CVE-2026-40404
Microsoft--Windows 10 Version 1607	Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability	2026-06-09	7.8	CVE-2026-40409
Microsoft--Windows 10 Version 1607	Improper access control in Microsoft Kinect allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-41092
Microsoft--Windows 10 Version 1607	Heap-based buffer overflow in Microsoft Windows DNS allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-41108
Microsoft--Windows 10 Version 1607	Concurrent execution using shared resource with improper synchronization ('race condition') in Function Discovery Service (fdwsd.dll) allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-42836
Microsoft--Windows 10 Version 1607	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-42905
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows RDP allows an unauthorized attacker to disclose information over a network.	2026-06-09	7.5	CVE-2026-42908
Microsoft--Windows 10 Version 1607	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-42911
Microsoft--Windows 10 Version 1607	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-42912
Microsoft--Windows 10 Version 1607	Integer underflow (wrap or wraparound) in Windows NT OS Kernel allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-42916
Microsoft--Windows 10 Version 1607	Integer underflow (wrap or wraparound) in Windows NT OS Kernel allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-42980
Microsoft--Windows 10 Version 1607	Use after free in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-42986

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft-- Windows 10 Version 1607	Improper link resolution before file access ('link following') in Winlogon allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-42989
Microsoft-- Windows 10 Version 1607	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5	CVE-2026-42992
Microsoft-- Windows 10 Version 1607	Improper link resolution before file access ('link following') in Windows Collaborative Translation Framework allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-45586
Microsoft-- Windows 10 Version 1607	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9	CVE-2026-45588
Microsoft-- Windows 10 Version 1607	Integer overflow or wraparound in Windows Internet (wininet.dll) allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-45592
Microsoft-- Windows 10 Version 1607	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-45596
Microsoft-- Windows 10 Version 1607	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-45598
Microsoft-- Windows 10 Version 1607	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-45601
Microsoft-- Windows 10 Version 1607	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-45603
Microsoft-- Windows 10 Version 1607	Use after free in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-45605
Microsoft-- Windows 10 Version 1607	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-45636
Microsoft-- Windows 10 Version 1607	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-45638
Microsoft-- Windows 10 Version 1607	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-45653
Microsoft-- Windows 10 Version 1607	Protection mechanism failure in Windows UEFI allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.8	CVE-2026-45656
Microsoft-- Windows 10 Version 1607	Protection mechanism failure in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2026-06-09	7.8	CVE-2026-45658
Microsoft-- Windows 10 Version 1607	Untrusted search path in Windows Storage allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-47648
Microsoft-- Windows 10 Version 1607	Protection mechanism failure in Windows Boot Manager allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9	CVE-2026-47656
Microsoft-- Windows 10 Version 1607	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9	CVE-2026-48568
Microsoft-- Windows 10 Version 1607	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9	CVE-2026-48570

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft-- Windows 10 Version 1607	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9	CVE-2026-48573
Microsoft-- Windows 10 Version 1607	Heap-based buffer overflow in Windows Media allows an unauthorized attacker to execute code locally.	2026-06-09	7.8	CVE-2026-48574
Microsoft-- Windows 10 Version 1607	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9	CVE-2026-48575
Microsoft-- Windows 10 Version 1607	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9	CVE-2026-48576
Microsoft-- Windows 10 Version 1607	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9	CVE-2026-48578
Microsoft-- Windows 10 Version 1607	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-48583
Microsoft-- Windows 10 Version 1607	Uncontrolled resource consumption in HTTP/2 allows an unauthorized attacker to deny service over a network.	2026-06-09	7.5	CVE-2026-49160
Microsoft-- Windows 10 Version 1809	Buffer over-read in Windows Projected File System Filter Driver allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-42828
Microsoft-- Windows 10 Version 1809	Buffer over-read in Windows Projected File System Filter Driver allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-42837
Microsoft-- Windows 10 Version 1809	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-42977
Microsoft-- Windows 10 Version 1809	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-42978
Microsoft-- Windows 10 Version 1809	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-42979
Microsoft-- Windows 10 Version 1809	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-42983
Microsoft-- Windows 10 Version 1809	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-42984
Microsoft-- Windows 10 Version 1809	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-42991
Microsoft-- Windows 10 Version 1809	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-44802
Microsoft-- Windows 10 Version 1809	Use after free in Windows SDK allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-45593
Microsoft-- Windows 10 Version 1809	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-45637
Microsoft-- Windows 10 Version 1809	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5	CVE-2026-48563

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft-- Windows 10 Version 21H2	Heap-based buffer overflow in Windows TCP/IP allows an unauthorized attacker to elevate privileges over an adjacent network.	2026-06-09	9.6	CVE-2026-42904
Microsoft-- Windows 10 Version 21H2	Out-of-bounds read in Windows Hyper-V allows an unauthorized attacker to execute code locally.	2026-06-09	8.4	CVE-2026-45641
Microsoft-- Windows 10 Version 21H2	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5	CVE-2026-42993
Microsoft-- Windows 10 Version 21H2	Time-of-check time-of-use (TOCTOU) race condition in Program Compatibility Assistant Service allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-45487
Microsoft-- Windows 10 Version 21H2	Use after free in Windows Bluetooth Port Driver allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-45640
Microsoft-- Windows 11 version 23H2	Use after free in Windows Kernel allows an unauthorized attacker to execute code over a network.	2026-06-09	9.8	CVE-2026-45657
Microsoft-- Windows 11 version 23H2	Integer underflow (wrap or wraparound) in Windows Performance Monitor allows an unauthorized attacker to execute code over a network.	2026-06-09	8.1	CVE-2026-42974
Microsoft-- Windows 11 version 23H2	Integer underflow (wrap or wraparound) in Windows Performance Monitor allows an unauthorized attacker to execute code over a network.	2026-06-09	8.1	CVE-2026-42981
Microsoft-- Windows 11 version 23H2	Improper authentication in Windows Cryptographic Services allows an unauthorized attacker to elevate privileges locally.	2026-06-09	8.4	CVE-2026-44810
Microsoft-- Windows 11 version 23H2	Out-of-bounds read in Windows Hyper-V allows an unauthorized attacker to execute code locally.	2026-06-09	8.2	CVE-2026-47652
Microsoft-- Windows 11 version 23H2	Concurrent execution using shared resource with improper synchronization ('race condition') in UI Automation Manager (uiamanager.dll) allows an authorized attacker to elevate privileges locally.	2026-06-09	7	CVE-2026-45597
Microsoft-- Windows 11 Version 24H2	Improper access control in Windows Administrator Protection allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.8	CVE-2026-42829
Microsoft-- Windows 11 Version 24H2	Out-of-bounds write in Windows Hotpatch Monitoring Service allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-42910
Microsoft-- Windows 11 Version 24H2	Use after free in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-44809
Microsoft-- Windows 11 Version 24H2	Access of resource using incompatible type ('type confusion') in Windows Kernel-Mode Drivers allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-45600
Microsoft-- Windows 11 Version 24H2	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9	CVE-2026-45654
Microsoft-- Windows 11 version 26H1	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-44804
Microsoft-- Windows 11 version 26H1	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-44807
Microsoft-- Windows 11 version 26H1	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-44808

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 11 version 26H1	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-44811
Microsoft--Windows 11 version 26H1	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-44813
Microsoft--Windows Narrator Braille	Untrusted search path in Windows Narrator Braille allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8	CVE-2026-48565
Microsoft--Windows Server 2012	Use after free in Windows Deployment Services allows an unauthorized attacker to execute code over a network.	2026-06-09	8.1	CVE-2026-42987
Microsoft--Windows Server 2012	Integer overflow or wraparound in Windows Kerberos allows an authorized attacker to execute code over an adjacent network.	2026-06-09	7.1	CVE-2026-47288
Microsoft--Windows Server 2016	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5	CVE-2026-47654
Microsoft--Windows Server 2022	Stack-based buffer overflow in Active Directory Domain Services allows an authorized attacker to execute code over a network.	2026-06-09	8.8	CVE-2026-45648
Missilesilo--KittyCatfish	KittyCatfish 2.2 plugin for WordPress contains an SQL injection vulnerability that allows unauthenticated attackers to read database contents by exploiting an unescaped GET parameter. Attackers can inject SQL code through the 'kc_ad' parameter in base.css.php or kittycatfish.php to extract sensitive database information using boolean-based blind or time-based blind techniques.	2026-06-09	8.2	CVE-2017-20246
moby--moby	Moby is an open source container framework. In Docker Engine prior to version 29.5.1, Docker Daemon versions 28.5.2 and prior, and Moby Daemon prior to version 2.0.0-beta.14, a race condition during docker cp mount setup allows a malicious container to redirect a bind mount target to an arbitrary host path, potentially overwriting host files or causing denial of service. This issue has been patched in Docker Engine version 29.5.1 and Moby Daemon version 2.0.0-beta.14.	2026-06-12	7.2	CVE-2026-42306
MongoDB--MongoDB	A use-after-free vulnerability exists in MongoDB Server's server-side JavaScript engine when converting BSON documents to JavaScript arrays. An authenticated user with read privileges who is able to run server-side JavaScript (for example, via \$where or \$function) can cause the server to access memory that has already been freed. This may result in disclosure of information from the mongod process memory or a denial of service through a server crash.	2026-06-12	8.8	CVE-2026-11933
MongoDB--MongoDB Server	The \$_internalApplyOplogUpdate aggregation pipeline stage can be used to execute a document diff containing a malformed binary diff to return memory out-of-bounds or crash the server. \$_internalApplyOplogUpdate can be executed by any authenticated user with access to the aggregate command.	2026-06-09	8.1	CVE-2026-9753
MongoDB--MongoDB Server	A vulnerability in MongoDB Server's BSON validation logic allows an unauthenticated user to crash the mongod process by sending a specially crafted message. The BSON validator's handling of certain nested binary data structures permits uncontrolled mutual recursion between validation functions, where each re-entry resets internal depth tracking.	2026-06-09	7.5	CVE-2026-9740
MongoDB--MongoDB Server	When OIDC authentication is enabled in configuration, clients may set specific values in the "mechanism" parameter of the "authenticate" command that lead to server crash. The authenticate command is accessible to unauthenticated clients, leading to pre-auth denial-of-service in affected product configurations.	2026-06-09	7.5	CVE-2026-9742
MOSK Information	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in MOSK Information Technologies Ltd. CBS	2026-06-09	9.8	CVE-2026-8025

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Technologies Ltd.--CBS Platform	Platform allows SQL Injection. This issue affects CBS Platform: through 09062026. NOTE: The vendor was contacted and it was learned that the product is not supported.			
nationalsecurityagency--ghidra	Ghidra 11.0 before 12.1 contains a SQL injection vulnerability in the changePassword() method of PostgresFunctionDatabase that fails to escape double quotes in usernames interpolated into ALTER ROLE statements. Authenticated attackers can inject SQL commands via crafted username parameters in PasswordChange network messages to escalate to PostgreSQL superuser privileges and gain full database control.	2026-06-10	8.8	CVE-2026-49498
nationalsecurityagency--ghidra	Ghidra before 12.1 contains an unsafe deserialization vulnerability in client-side Shared-Project RMI connection code that allows unauthenticated remote code execution. Attackers can craft a malicious project file with a ghidra:// URL that, when opened via File â Open Project, deserializes untrusted objects using a Jython 2.7.4 gadget chain to execute arbitrary commands.	2026-06-10	8.8	CVE-2026-52751
nationalsecurityagency--ghidra	Ghidra before 12.1 contains an authentication bypass vulnerability in PKIAuthenticationModule.authenticate() that allows any user with a valid CA-signed certificate to impersonate other users by presenting their public certificate with a null signature. Attackers can escalate privileges, modify repository access controls, exfiltrate shared reverse engineering databases, and permanently compromise server integrity.	2026-06-10	8.8	CVE-2026-52754
nationalsecurityagency--ghidra	Ghidra before 12.1 contains a SQL injection vulnerability in BSim filter types that concatenate user-supplied values directly into SQL queries without escaping or parameterization. Remote attackers can inject arbitrary SQL via the BSim network query protocol to read, modify, or delete data in the PostgreSQL database.	2026-06-10	8.8	CVE-2026-52758
nationalsecurityagency--ghidra	Ghidra before 12.1 contains a command injection vulnerability in URL annotation handling on Windows where cmd.exe metacharacters are not properly escaped. Attackers can execute arbitrary commands under the Ghidra user's privileges by embedding malicious URLs in program comments that victims click.	2026-06-10	7.8	CVE-2026-52750
nationalsecurityagency--ghidra	Ghidra before 12.0.2 contains a path traversal vulnerability in the extension installer that fails to validate ZIP entry names during extraction. Attackers can craft malicious extensions with traversal sequences like ../ in filenames to write arbitrary files outside the intended directory, enabling code execution.	2026-06-10	7.8	CVE-2026-52752
nationalsecurityagency--ghidra	Ghidra before 12.0.4 contains a path traversal vulnerability in the theme import functionality that allows attackers to write files outside the intended theme directory. Attackers can craft malicious theme ZIP files with traversal sequences in filenames to execute arbitrary code or modify sensitive files like .bashrc or .ssh/authorized_keys.	2026-06-10	7.8	CVE-2026-52755
Naxclow--Smart Doorbell X3	Naxclow devices use a uniform request-signing scheme based on a hard-coded, platform-wide salt embedded in every firmware image. Once this salt is recovered from any device, an attacker can generate valid signatures for arbitrary device or account operations due to the absence of per-device keys, server-side nonce tracking, or replay protections. Combined with the system's use of plain HTTP for control-plane traffic, the construction enables broad request forgery and impersonation across the platform.	2026-06-12	9.8	CVE-2026-28742
Naxclow--Smart Doorbell X3	A flaw in Naxclow's platform's onboarding workflow allows an attacker to replay a confirm-then-bind sequence to silently reassign a device to an arbitrary account. Because the affected endpoints validate request signatures but do not confirm legitimate ownership, an attacker with any account can take over a device without user interaction while the device remains online and unaware.	2026-06-12	8.8	CVE-2026-42947
Naxclow--Smart Doorbell X3	Naxclow devices use a server-side, per-device relay credential that never rotates and is re-issued to the device on each boot. Because this credential remains valid indefinitely and cannot be reset or revoked by the legitimate owner, any party that obtains it through any exposure path can maintain	2026-06-12	8.1	CVE-2026-50101

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	persistent access to the device's relay channel. This enables long-term impersonation or interception, even after factory resets or re-onboarding.			
Naxclow--Smart Doorbell X3	The Naxclow platform API that returns device relay registration details exposes a persistent credential without verifying that the requester is the legitimate device or owner. An actor able to present a platform-valid request signature can retrieve credentials for arbitrary devices and register on the relay as that device, enabling interception and disruption of its communications.	2026-06-12	7.5	CVE-2026-50108
Nefteprodukttekhnik LLC--BUK TS-G Gas Station Automation System	Nefteprodukttekhnik BUK TS-G Gas Station Automation System 2.9.1 through 2.10.2 on Linux contains an Improper Authentication vulnerability (CWE-287) in the system configuration module. The /php/ajax-login.php endpoint returns userid=1 (administrator) in response to any HTTP POST request that supplies arbitrary credentials (e.g., action=dologin&login=<any_value>&pwd=<any_value>), and subsequent privileged endpoints under /php/ajax-main.php and /modules/* do not validate a server-side session. A remote unauthenticated attacker can invoke any administrative action exposed by the configuration module, including reading and modifying user rules, fuel tank gauges, fuel dispensers, relays, cash registers, bank terminals, fuel cards, price and customer displays, cash collection, and pricing rules.	2026-06-13	9.8	CVE-2026-12183
nesquena--hermes-webui	Hermes WebUI before version 0.51.358 contains an improper access control vulnerability that allows unauthenticated remote attackers to hijack initial setup by submitting the _set_password parameter to the settings API endpoint without any network origin restriction. Attackers on any reachable network can send a POST request to the settings endpoint during the first-run setup window to persist an arbitrary password hash, obtain a valid session cookie, and lock out the legitimate operator from their own instance.	2026-06-11	9.4	CVE-2026-49973
nesquena--hermes-webui	Hermes WebUI before version 0.51.311 contains a remote code execution vulnerability that allows authenticated attackers to execute arbitrary commands by placing malicious executable Git configuration in a workspace repository's .git/config file. Attackers can exploit Git subprocess invocations in api/workspace_git.py through vectors such as core.fsmonitor during git status, protocol.ext.allow with ext::remotes during git fetch, credential.helper, core.askPass, core.gitProxy, or inherited environment variables including GIT_SSH_COMMAND to achieve arbitrary command execution on the host running the application.	2026-06-09	8.8	CVE-2026-49959
nesquena--hermes-webui	Hermes WebUI before version 0.51.296 contains a workspace boundary bypass vulnerability that allows authenticated attackers to circumvent blocked-root path checks by exploiting an early return in the SSH/remote terminal profile workspace resolution logic within _remote_terminal_workspace_candidate(). Attackers can configure a remote terminal working directory to a system directory such as /etc, causing the workspace resolution path to accept it as a trusted local workspace root before the _is_blocked_workspace_path() guard executes, enabling read access to local system files through workspace file-read helpers.	2026-06-09	7.7	CVE-2026-49957
Netcad Software Inc.--E-mar	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Netcad Software Inc. E-Ä°mar allows SQL Injection. This issue affects E-Ä°mar: from 2.10.1.0 before 3.0.2.	2026-06-09	9.8	CVE-2026-7486
netty--netty	Netty is a network application framework for development of protocol servers and clients. In netty-handler prior to versions 4.1.135.Final and 4.2.15.Final, an attacker can bypass IPv6 subnet rules due to an incorrect masking operation in IpSubnetFilterRule.compareTo(). Valid public IP addresses can bypass the restrictions. Versions 4.1.135.Final and 4.2.15.Final patch the issue.	2026-06-11	8.1	CVE-2026-44249
netty--netty	Netty is a network application framework for development of protocol servers and clients. Prior to versions 4.1.135.Final and 4.2.15.Final, Netty's	2026-06-12	8.7	CVE-2026-45674

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	DnsResolveContext fails to validate the origin (bailiwick) of CNAME records in DNS responses. Versions 4.1.135.Final and 4.2.15.Final patch the issue.			
netty--netty	Netty is a network application framework for development of protocol servers and clients. Prior to versions 4.1.135.Final and 4.2.15.Final, Netty's `DnsResolveContext` insufficiently validates the bailiwick of NS records, enabling DNS Cache Poisoning. An attacker controlling an authoritative name server for a subdomain can poison the cache for parent domains (like `.co.uk`). In `io.netty.resolver.dns.DnsResolveContext.AuthoritativeNameServerList#add` method accepts any NS record from the AUTHORITY section as long as the record's name is a suffix of the questionName. Subsequently, the `handleWithAdditional` method caches the associated A records from the ADDITIONAL section directly into the `authoritativeDnsServerCache` under the parent domain's key. This bypasses standard bailiwick rules, where a server authoritative for a subdomain should not be trusted to provide authoritative records for its parent. The poisoned cache is then used for all future resolutions under the parent domain's key. Versions 4.1.135.Final and 4.2.15.Final patch the issue.	2026-06-12	8.7	CVE-2026-47691
netty--netty	Netty is a network application framework for development of protocol servers and clients. In netty-codec-redis prior to versions 4.1.135.Final and 4.2.15.Final, an attacker can cause DoS by sending a crafted Redis payload with deeply nested arrays. This forces the server to allocate a massive number of state objects and collections, leading to memory exhaustion and an OutOfMemoryError. Versions 4.1.135.Final and 4.2.15.Final patch the issue.	2026-06-11	7.5	CVE-2026-44250
netty--netty	Netty is a network application framework for development of protocol servers and clients. In netty-codec-redis prior to versions 4.1.135.Final and 4.2.15.Final, an attacker can cause DoS by sending crafted Redis payloads across multiple connections without `\r\n`. This exhausts the server's direct memory pool (OutOfDirectMemoryError), preventing legitimate connections from being processed. Versions 4.1.135.Final and 4.2.15.Final patch the issue.	2026-06-11	7.5	CVE-2026-44890
netty--netty	Netty is a network application framework for development of protocol servers and clients. Prior to version 4.2.15.Final, the default configuration of the `Http3ConnectionHandler` in the Netty HTTP/3 codec lacks an enforced maximum header size limit. When a peer does not explicitly specify `HTTP3_SETTINGS_MAX_FIELD_SECTION_SIZE`, the implementation defaults to an unbounded limit. This insecure default configuration allows a malicious client or server to send an enormous number of headers, leading to a memory exhaustion Denial of Service via an `OutOfMemoryError`. Version 4.2.15.Final contains a patch.	2026-06-12	7.5	CVE-2026-44892
netty--netty	Netty is a network application framework for development of protocol servers and clients. In netty-codec-haproxy prior to versions 4.1.135.Final and 4.2.15.Final, when decoding a PP2_TYPE_SSL TLV, HAProxyMessage.readNextTLV() first calls `header.retainedSlice(header.readerIndex(), length)` and only then reads the 1-byte client field and 4-byte verify field. If the attacker sets the TLV length below 5, the subsequent readByte/readInt throws IndexOutOfBoundsException. HAProxyMessageDecoder only catches HAProxyProtocolException around this call, so the IOOBE propagates and the retained slice on the pooled cumulation buffer is never released. Versions 4.1.135.Final and 4.2.15.Final patch the issue.	2026-06-12	7.5	CVE-2026-44893
netty--netty	Netty is a network application framework for development of protocol servers and clients. NoQuicTokenHandler is the tokenHandler used when the application does not set one. Prior to version 4.2.15.Final, its writeToken() returns false (server will not send Retry - acceptable), but validateToken() unconditionally `return 0`. In QuicheQuicServerCodec.handlePacket(), a non-negative return from validateToken() is interpreted as 'token is valid, ODCID starts at offset 0',	2026-06-12	7.5	CVE-2026-44894

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	causing the server to call <code>quiche_accept</code> as if the client's address had been validated by a Retry round-trip. Per RFC 9000 §8.1, a validated address lifts the 3 rd — anti-amplification send limit. Thus any attacker who includes ANY non-empty token bytes in an Initial packet - with a spoofed victim source IP - causes the Netty server to treat the victim as validated and reflect full-size handshake flights (certificates, etc.) toward it without the 3 rd — cap. The correct 'no token handler' semantics would be to return -1 (invalid) so the normal un-validated path and amplification limit apply. Version 4.2.15.Final patches the issue.			
netty--netty	Netty is a network application framework for development of protocol servers and clients. Prior to versions 4.1.135.Final and 4.2.15.Final, <code>SslClientHelloHandler.decode()</code> reads the 24-bit TLS handshake length and, when the ClientHello does not fit in the first record, eagerly allocates <code>`ctx.alloc().buffer(handshakeLength)`</code> (line 161). The guard at line 140 is <code>`handshakeLength > maxClientHelloLength && maxClientHelloLength != 0`</code> , and the commonly-used <code>SniHandler/AbstractSniHandler</code> constructors (<code>SniHandler(Mapping)</code> , <code>SniHandler(AsyncMapping)</code> , <code>AbstractSniHandler()</code>) pass <code>maxClientHelloLength=0</code> and <code>handshakeTimeoutMillis=0</code> , so the length guard is disabled and no timeout is scheduled. A 16 MiB request exceeds the default pooled chunk size and becomes a huge/unpooled allocation performed immediately. The buffer is retained in the handler until the channel closes. Versions 4.1.135.Final and 4.2.15.Final patch the issue.	2026-06-12	7.5	CVE-2026-45416
netty--netty	Netty is a network application framework for development of protocol servers and clients. In versions of <code>netty-transport-sctp</code> prior to 4.1.135.Final and 4.2.15.Final, for each non-complete <code>SctpMessage</code> fragment the handler does <code>`fragments.put(streamId, Unpooled.wrappedBuffer(frag, byteBuf))`</code> , wrapping the previous accumulator and the new slice into a <code>*new*</code> <code>CompositeByteBuf</code> every time. After N fragments the accumulator is an N-deep chain of composites, each holding references and component arrays; <code>readableBytes()/getBytes()</code> on the final buffer recurse N levels. There is no limit on N, on total bytes, or on the number of stream identifiers an attacker can open (each gets its own map entry). A peer that never sets the <code>`complete`</code> flag can grow this structure indefinitely from tiny 1-byte DATA chunks. Versions 4.1.135.Final and 4.2.15.Final patch the issue.	2026-06-12	7.5	CVE-2026-46340
netty--netty	Netty is a network application framework for development of protocol servers and clients. Prior to version 4.2.15.Final, a memory exhaustion vulnerability in the Netty HTTP/3 codec allows the creation of an infinite number of blocked streams, which can cause OOM error. Version 4.2.15.Final patches the issue.	2026-06-12	7.5	CVE-2026-48748
netty--netty	Netty is a network application framework for development of protocol servers and clients. Prior to versions 4.1.135.Final and 4.2.15.Final, <code>SimpleTrustManagerFactory.engineGetTrustManagers()</code> and related paths wrap any user-supplied plain <code>X509TrustManager</code> in <code>X509TrustManagerWrapper</code> , which extends <code>X509ExtendedTrustManager</code> but implements the 3-arg <code>checkServerTrusted(chain, authType, SSLEngine)</code> by discarding the <code>SSLEngine</code> and calling the 2-arg delegate. Because the object now IS an <code>X509ExtendedTrustManager</code> , neither <code>SunJSE</code> 's internal <code>AbstractTrustManagerWrapper</code> nor Netty's own <code>OpenSslX509TrustManagerWrapper</code> will re-wrap it to add endpoint-identification. Consequently, even though Netty 4.2 sets <code>endpointIdentificationAlgorithm="HTTPS"</code> by default, a client built with <code>`SslContextBuilder.forClient().trustManager(somePlainX509TrustManager)`</code> performs no hostname verification at all. Versions 4.1.135.Final and 4.2.15.Final patch the issue.	2026-06-12	7.5	CVE-2026-50010
netty--netty	Netty is a network application framework for development of protocol servers and clients. Prior to versions 4.1.135.Final and 4.2.15.Final, <code>RedisArrayAggregator</code> pre-allocates <code>ArrayList</code> with initial capacity equal to	2026-06-12	7.5	CVE-2026-50011

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the RESP array element count declared in an array header. That count is taken from the wire before the corresponding child messages exist. A small malicious header can claim a huge initial capacity. Versions 4.1.135.Final and 4.2.15.Final patch the issue.			
nezhahq--nezha	Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. From version 1.4.0 to before version 2.0.8, a RoleMember user can create a scheduled cron task with Cover=CronCoverAll, Servers=[] and an arbitrary Command. At every tick of the scheduler, the dashboard pushes that command to every server in the global ServerShared map - including servers that belong to other tenants (admin's servers, other members' servers). Each agent runs the command and returns the output, which is then sent to the attacker's own NotificationGroup attacker-controlled webhook. This issue has been patched in version 2.0.8.	2026-06-12	9.9	CVE-2026-46716
nezhahq--nezha	Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. Prior to version 2.0.13, fallbackToFrontend in the dashboard's NoRoute handler treats any URL whose raw string starts with /dashboard as an admin-frontend asset request. The check uses strings.HasPrefix, not a path-segment match, so the input /dashboard../data/config.yaml is accepted; strings.TrimPrefix leaves ../data/config.yaml; and path.Join("admin-dist", "../data/config.yaml") normalizes to data/config.yaml - which os.Stat finds and http.ServeFile returns. No authentication required. This issue has been patched in version 2.0.13.	2026-06-12	9.1	CVE-2026-53519
nezhahq--nezha	Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. From version 1.4.0 to before version 2.0.8, nezha's dashboard supports two user roles: RoleAdmin (Role==0) and RoleMember (Role==1). The notification routes POST /api/v1/notification and PATCH /api/v1/notification/:id are wired through commonHandler rather than adminHandler - so a RoleMember user can call them. These handlers synchronously Send() an HTTP request to a user-controlled URL and reflect the entire response body (no size limit) back to the caller on any non-2xx response. This issue has been patched in version 2.0.8.	2026-06-12	7.7	CVE-2026-46717
nezhahq--nezha	Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. From version 1.4.0 to before version 2.0.8, a RoleMember can fire other users' cron tasks via AlertRule.FailTriggerTasks (no ownership check). This issue has been patched in version 2.0.8.	2026-06-12	7.1	CVE-2026-47120
nezhahq--nezha	Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. From version 0.20.0 to before version 2.0.12, authenticated agents can forge service-monitor results for other users' services. This issue has been patched in version 2.0.12.	2026-06-12	7.1	CVE-2026-48119
nezhahq--nezha	Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. From version 1.0.0 to before version 2.0.14, cross-site GET request can trigger stored cron commands on a victim's agents. This issue has been patched in version 2.0.14.	2026-06-12	7.1	CVE-2026-49396
NginxProxyManager--nginx-proxy-manager	Nginx Proxy Manager versions 2.9.14 through 2.15.1, fixed in commit a5db5ed, contain an authenticated remote code execution vulnerability via OS command injection in the setupCertbotPlugins() function in backend/setup.js, allowing attackers with certificates:manage permission to execute arbitrary commands by storing a malicious payload in the dns_provider_credentials field. The user-controlled dns_provider_credentials value is interpolated directly into a shell command executed via child_process.exec() without sanitization or escaping, causing the injected command to execute upon backend restart.	2026-06-08	7.5	CVE-2026-40519
nimiq--core-rs-albatross	Nimiq is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. Prior to version 1.4.0, in handle_dht_get(), the DhtResults accumulator is only initialized when the first DHT record passes verification. If the first record fails (from a malicious DHT node), DhtResults is never created, and all subsequent valid	2026-06-09	7.5	CVE-2026-46541

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	records are discarded with "DHT inconsistent state" errors. This issue has been patched in version 1.4.0.			
nimiq--core-rs-albatross	Nimiq is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. Prior to version 1.5.0, a remote, unauthenticated denial-of-service vulnerability in MerkleRadixTrie::put_chunk allows any state-sync peer to crash any node performing state synchronization (freshly joining nodes and recovering nodes). This issue has been patched in version 1.5.0.	2026-06-09	7.5	CVE-2026-46545
NVIDIA--DALI	NVIDIA DALI contains a vulnerability in a component where an attacker could cause a heap-based buffer overflow. A successful exploit of this vulnerability might lead to code execution, data tampering, denial of service, and information disclosure.	2026-06-09	7.3	CVE-2026-24180
NVIDIA--DALI	NVIDIA DALI contains a vulnerability in a component where an attacker could cause an improper index validation. A successful exploit of this vulnerability might lead to code execution, data tampering, denial of service, and information disclosure.	2026-06-09	7.3	CVE-2026-24181
Ollie Armstrong--Simply Poll	Simply Poll 1.4.1 plugin for WordPress contains an SQL injection vulnerability that allows unauthenticated attackers to extract database information by injecting SQL code through the 'pollid' POST parameter. Attackers can send requests to the admin-ajax.php endpoint with the 'spAjaxResults' action and malicious 'pollid' values to execute arbitrary SQL queries and read sensitive data from the WordPress database.	2026-06-09	8.2	CVE-2016-20062
Omnissa--Omnissa Workspace ONE Assist for macOS	Omnissa Workspace ONE® Assist for macOS contains a Local Privilege Escalation Vulnerability.	2026-06-09	7.8	CVE-2026-22926
open-metadata--OpenMetadata	OpenMetadata is a unified metadata platform. Prior to version 1.12.4, a non-admin SSO user can trigger a TEST_CONNECTION workflow for a Database Service and receive, in the HTTP 201 response of POST /api/v1/automations/workflows, both the cleartext database password in request.connection.config.password and the ingestion bot JWT in openMetadataServerConnection.securityConfig.jwtToken. The leaked ingestion-bot token can then be reused as Authorization: Bearer <jwt> to access sensitive service APIs with bot-level privileges. This issue has been patched in version 1.12.4.	2026-06-08	8.3	CVE-2026-46481
openbullet--openbullet2	OpenBullet2 through version 0.3.2 contains an authentication bypass vulnerability in the API key authentication middleware that allows unauthenticated attackers to gain admin access by supplying an empty X-API-Key header value. Attackers can exploit the middleware's comparison of the supplied header against an empty AdminApiKey default string to access the admin console and all API endpoints without valid credentials.	2026-06-08	9.8	CVE-2026-25555
openbullet--openbullet2	OpenBullet2 through version 0.3.2 contains a path traversal vulnerability in the wordlist endpoint that allows authenticated attackers to perform arbitrary file read, write, and delete operations by supplying unsanitized absolute paths to the upload handler and wordlist functions. Attackers can chain the file write and delete primitives to achieve remote code execution by manipulating critical system files such as /etc/passwd, with full system impact since the application runs as root by default.	2026-06-08	8.8	CVE-2026-25559
openbullet--openbullet2	OpenBullet2 through version 0.3.2 contains a remote code execution vulnerability that allows authenticated users to execute arbitrary commands by uploading script files (.bat.ps1.sh) through the FileProxySource proxy loading feature. Attackers can upload malicious script files as proxy sources, causing the server to execute the scripts and return output as proxy lines, resulting in arbitrary command execution on the host as the process user.	2026-06-08	8.8	CVE-2026-25855
openbullet--openbullet2	OpenBullet2 through version 0.3.2 contains an authenticated remote code execution vulnerability that allows authenticated users to execute arbitrary C# code on the server host by creating or modifying job configurations. Attackers can leverage the plain C# execution mode, which	2026-06-08	8.8	CVE-2026-25856

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	lacks reference filtering or API restrictions, to access the file system, spawn processes, and invoke arbitrary .NET APIs as the process user.			
OpenClaw-- OpenClaw	OpenClaw before 2026.5.27 contains a state mutation vulnerability in node pairing reconnection that allows paired nodes to confuse approval scope decisions. Attackers can exploit reconnection logic to restore or present broader node authority than intended, potentially bypassing approval restrictions.	2026-06-12	9.8	CVE-2026-53838
OpenClaw-- OpenClaw	OpenClaw before 2026.5.12 contains a shell option parsing vulnerability that allows combined POSIX shell flags to bypass exec revalidation checks. Attackers can exploit this by using combined shell options to execute inline shell content without intended allowlist validation, potentially enabling unauthorized command execution when the affected feature is enabled.	2026-06-11	8.8	CVE-2026-53806
OpenClaw-- OpenClaw	OpenClaw before 2026.5.6 contains an authorization bypass vulnerability in Telegram interactive callbacks that allows authenticated users to skip commands.allowFrom validation. Attackers can invoke affected callbacks to mark themselves as authorized senders before allowlist checks are applied, triggering command behavior outside configured Telegram sender restrictions.	2026-06-11	8.8	CVE-2026-53807
OpenClaw-- OpenClaw	OpenClaw before 2026.5.18 contains a code execution vulnerability where marketplace runtime extension metadata can redirect loading toward unscanned package payloads. Attackers with trusted operator access can manipulate extension metadata to load plugin code outside reviewed package entry points, bypassing security scanning.	2026-06-11	8.8	CVE-2026-53810
OpenClaw-- OpenClaw	OpenClaw before 2026.5.7 contains a privilege escalation vulnerability in the Matrix allowFrom feature that allows authenticated accounts to match policy entries through mutable display name metadata. Attackers with the ability to change display names can receive agent access intended for another Matrix identity, potentially gaining unauthorized permissions depending on operator configuration.	2026-06-11	8.8	CVE-2026-53811
OpenClaw-- OpenClaw	OpenClaw before 2026.5.20 contains a privilege escalation vulnerability where hook-triggered agent runs incorrectly receive owner-scoped MCP loopback authority instead of hook-appropriate scope. Attackers with a valid hook token can exploit the /hooks/agent endpoint to cause spawned CLI runtimes to access or invoke owner-only MCP tools, potentially executing privileged actions like persistent cron state modifications.	2026-06-11	8.3	CVE-2026-53814
OpenClaw-- OpenClaw	OpenClaw before 2026.5.22 contains a locality validation vulnerability in Control UI pairing that allows attackers with network access to spoof locality information and obtain durable admin-capable device tokens. Attackers can exploit insufficient locality-derived trust validation to convert temporary shared access into persistent administrative credentials that survive token rotation.	2026-06-11	8.8	CVE-2026-53817
OpenClaw-- OpenClaw	OpenClaw before 2026.5.27 contains an arbitrary code execution vulnerability in skill install flows where workspace .env files can override the Homebrew executable selection. Attackers with access to trusted operator workspaces can execute unintended Homebrew-compatible executables during skill setup to compromise the system.	2026-06-11	8.8	CVE-2026-53819
OpenClaw-- OpenClaw	OpenClaw before 2026.5.18 accepts WebSocket client-declared operator scopes before binding to server-approved pairing or trusted-proxy authorization baseline. Unpaired or restricted trusted-proxy Control UI clients can obtain cached operator.admin authority on live WebSocket connections to execute admin-gated Gateway RPCs.	2026-06-12	8.8	CVE-2026-53821
OpenClaw-- OpenClaw	OpenClaw before 2026.5.18 contains a command injection vulnerability where shell wrapper argv could change between approval and execution. Attackers can rebuild command arguments after allowlist approval to execute unapproved command shapes, potentially bypassing security controls.	2026-06-12	8.8	CVE-2026-53822
OpenClaw-- OpenClaw	OpenClaw before 2026.5.3 contains a privilege escalation vulnerability in the allowFrom feature that binds to mutable Slack display names. Attackers with Slack account access can change display name metadata to	2026-06-12	8.1	CVE-2026-53823

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	match policy entries, potentially gaining unauthorized agent access intended for other identities.			
OpenClaw-- OpenClaw	OpenClaw before 2026.5.6 contains an authorization bypass vulnerability in native command handling that allows authenticated senders to execute owner-only commands without proper policy enforcement. Attackers can trigger native command handling to bypass the configured owner-command access control, potentially executing privileged commands from unauthorized users.	2026-06-12	8.8	CVE-2026-53828
OpenClaw-- OpenClaw	OpenClaw before 2026.5.18 contains an approval display truncation vulnerability allowing authenticated users to hide command suffixes from approvers. Attackers can submit oversized exec commands with benign prefixes and malicious suffixes to execute unauthorized operations after approval.	2026-06-12	8	CVE-2026-53829
OpenClaw-- OpenClaw	OpenClaw before 2026.5.18 contains a policy enforcement vulnerability in system.run safe-bin allowlist validation that allows shell expansion to modify command interpretation on POSIX nodes. Authenticated operators can exploit shell metacharacters in approved commands to read unintended node-local files and expose sensitive configuration data.	2026-06-12	8.3	CVE-2026-53831
OpenClaw-- OpenClaw	OpenClaw before 2026.5.12 contains an allowlist bypass vulnerability in PowerShell encoded-command handling that allows attackers to execute encoded commands using abbreviated flag aliases not recognized by the allowlist parser. Remote authenticated operators can bypass execution allowlist checks by using unrecognized encoded-command alias forms to execute arbitrary PowerShell content.	2026-06-12	8.8	CVE-2026-53836
OpenClaw-- OpenClaw	OpenClaw before 2026.5.18 contains a server-side request forgery vulnerability in browser control that allows authenticated users to bypass private-network navigation checks through Playwright act interactions. Attackers can trigger navigation to private-network targets via action-triggered redirects and subsequently read restricted page content using browser evaluation capabilities.	2026-06-11	7.7	CVE-2026-53812
OpenClaw-- OpenClaw	OpenClaw before 2026.4.25 contains a path traversal vulnerability in memory-core artifact loading where workspace state influences local package root resolution. Attackers with access to affected workspaces can load memory-core artifacts from unintended local locations, potentially executing malicious code or accessing sensitive data.	2026-06-11	7.8	CVE-2026-53813
OpenClaw-- OpenClaw	OpenClaw before 2026.5.18 contains an insufficient provenance validation vulnerability in node event handling that allows paired nodes to forge exec lifecycle events without system.run authorization. A malicious or compromised paired node can send crafted node.event messages to the gateway, steering target sessions into exec-event paths that expose capabilities the reduced node surface should not provide.	2026-06-11	7.2	CVE-2026-53816
OpenClaw-- OpenClaw	OpenClaw before 2026.5.18 contains an identity header validation vulnerability allowing local same-host callers to forge trusted-proxy identity headers. Attackers with access to the proxy-facing Gateway port can supply forged identity headers to assume operator identity and potentially escalate privileges.	2026-06-12	7.7	CVE-2026-53832
OpenClaw-- OpenClaw	OpenClaw before 2026.4.29 contains an authorization bypass vulnerability in the QqBot streaming command that allows authenticated senders to mutate configuration without explicit allowFrom restrictions. Attackers can modify QqBot streaming configuration outside intended admin policy by reaching the affected command without non-wildcard allowlist entry requirements.	2026-06-12	7.7	CVE-2026-53833
OpenClaw-- OpenClaw	OpenClaw before 2026.4.27 contains an authorization bypass vulnerability in QqBot pre-dispatch slash commands that allows authenticated senders to skip allowFrom policy checks. Attackers can invoke slash commands before configured access control policies are applied, potentially triggering command handling from blocked senders depending on operator configuration.	2026-06-12	7.5	CVE-2026-53834

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openemr--openemr	OpenEMR is a free and open source electronic health records and medical practice management application. Prior to version 8.0.0.1, a stored cross-site scripting vulnerability in the prescription CSS/HTML multi-print feature allows a patient portal user to execute arbitrary JavaScript in a clinician's browser session. Patient demographic fields (name, address) are rendered without output encoding in multiprintcss_header(), and portal patients can write attacker-controlled HTML directly into patient_data by calling the PUT api/patient/:num endpoint, which bypasses the intended audit review workflow. Because the XSS fires in the clinician's authenticated session on the main OpenEMR interface, the attacker can access CSRF tokens, session data, and perform actions as the clinician - crossing the patient-to-clinician trust boundary. This issue has been patched in version 8.0.0.1.	2026-06-09	7.7	CVE-2026-46518
Oracle Corporation--PeopleSoft Enterprise PeopleTools	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Updates Environment Management). Supported versions that are affected are 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-11	9.8	CVE-2026-35273
patriksimek--vm2	vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.4, by combining Buffer.call.call({.__lookupGetter__, Buffer, "__proto__"}, Buffer.call.call({.__lookupSetter__, Buffer, "__proto__"}, and Node.js's ERR_INVALID_ARG_TYPE Error, the host's TypeError constructor can be obtained, which allows the escape from the sandbox. This allows attackers to run arbitrary code. This issue has been patched in version 3.11.4.	2026-06-12	10	CVE-2026-47131
patriksimek--vm2	vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.4, the fix for GHSA-8hg8-63c5-gwmx (CVE-2023-37903) introduced a check in nodevm.js line 263 that blocks the combination nesting: true + require: false. However, the check uses strict equality (options.require === false), which is trivially bypassed by omitting the require option entirely. When require is not specified, options.require is undefined, not false. The strict equality check fails, so the security guard is skipped. Immediately after (line 280), the destructuring default require: requireOpts = false assigns requireOpts = false, producing the exact configuration the patch was designed to prevent. This issue has been patched in version 3.11.4.	2026-06-12	10	CVE-2026-47137
patriksimek--vm2	vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.4, NodeVM blocks several dangerous Node.js builtins such as module, worker_threads, cluster, vm, repl, and inspector. However, the denylist misses process and inspector/promises. Both can be used from sandboxed code to reach host-side execution primitives. This allows sandboxed code to bypass the intended builtin restrictions and execute code in the host process. This issue has been patched in version 3.11.4.	2026-06-12	10	CVE-2026-47140
patriksimek--vm2	vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.4, VM2 suffers from a sandbox breakout vulnerability. This allows attackers to write code which can escape from the VM2 sandbox and execute arbitrary commands on the host system. This issue has been patched in version 3.11.4.	2026-06-12	10	CVE-2026-47208
patriksimek--vm2	vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.4, a sandbox escape vulnerability in vm2 allows arbitrary code execution in the host process when untrusted code is executed with async support on runtimes exposing WebAssembly JSPI (WebAssembly.promising / WebAssembly.Suspending). In the tested configuration, a JSPI-backed Promise can reach Promise.prototype.finally() in a way that bypasses the expected Promise-species hardening and exposes a host-originated rejection object to attacker-controlled species logic, breaking the sandbox boundary. This issue has been patched in version 3.11.4.	2026-06-12	9.8	CVE-2026-47210
patriksimek--vm2	vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.4, Symbol.for override in setup-sandbox.js only intercepts 2 of 9 dangerous	2026-06-12	8.7	CVE-2026-47135

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Node.js cross-realm symbols. Combined with the bridge's set/defineProperty/deleteProperty traps having no isDangerousCrossRealmSymbol key check, sandbox code can obtain real cross-realm symbols, write them to host objects, and control host-side behavior - verified with a full util.promisify hijack chain. This issue has been patched in version 3.11.4.			
patriksimek--vm2	vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.4, NodeVM supports excluding public network builtins from the wildcard builtin option. With this configuration direct access to http, https, http2, net, dgram, tls, dns, and dns/promises is blocked. However, Node.js also exposes underscored internal HTTP builtins such as _http_client and _http_server. These are not blocked when the public modules are excluded. Sandboxed code can use these internal builtins to make outbound HTTP requests and open listening HTTP sockets even though the public network modules are denied. This issue has been patched in version 3.11.4.	2026-06-12	8.6	CVE-2026-47139
patriksimek--vm2	vm2 is an open source vm/sandbox for Node.js. Prior to version 3.11.4, the BaseHandler.set trap in bridge.js (line 1231) ignores the receiver parameter and unconditionally writes to the host target object. Per the Proxy set trap specification, when receiver !== proxy (e.g., when a child object inherits from the proxy via Object.create), the property assignment should create an own property on the receiver, not on the proxy target. The current implementation always calls otherReflectSet(object, key, value) against the host target, causing all inherited property writes to leak through to the host object. This bug provides an alternative attack vector for writing dangerous cross-realm Symbol keys (e.g., nodejs.util.promisify.custom) to host objects, bypassing any future per-trap isDangerousCrossRealmSymbol guard on the direct set path. This issue has been patched in version 3.11.4.	2026-06-12	8.6	CVE-2026-47209
PbootCMS--PbootCMS	A security flaw has been discovered in PbootCMS up to 3.2.12. This vulnerability affects the function retrieve of the file apps/home/controller/MemberController.php of the component Password Handler. The manipulation of the argument username/password/email/checkcode results in weak password recovery. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	2026-06-12	7.3	CVE-2026-12066
PerryTS--perry	Perry before 0.5.1159 contains a path traversal vulnerability that allows a malicious build server to write arbitrary content to any location writable by the running process by supplying unsanitized path components in the artifact_name field of ArtifactReady WebSocket messages. Attackers controlling the server URL can deliver traversal payloads through the artifact_name or download_path fields, causing the client to overwrite sensitive files or expose arbitrary local files to an attacker-accessible location.	2026-06-11	8.1	CVE-2026-53777
php--frankenphp	FrankenPHP is a modern application server for PHP. From version 1.11.2 to before version 1.12.3, the splitPos() function in cgi.go misuses golang.org/x/text/search with search.IgnoreCase when the request path contains a non-ASCII byte. Two distinct flaws in that fallback let an attacker mislead FrankenPHP into treating a non-.php file as a .php script. In any deployment where the attacker can place content into a file served by FrankenPHP (uploads, file storage, etc.), this can be escalated to remote code execution by crafting a URL whose path triggers either flaw. This issue has been patched in version 1.12.3.	2026-06-10	8.1	CVE-2026-45062
pi-hole--FTL	Pi-hole FTL is the core engine of the Pi-hole network-level advertisement and tracker blocker. Prior to version 6.6.1, Pi-hole FTL contains a race condition vulnerability in the HTTP session management subsystem, introduced with the v6.0 rewrite of the embedded CivetWeb-based web server. This issue has been patched in version 6.6.1.	2026-06-10	8.8	CVE-2026-44693

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pipecat-ai--pipecat	Pipecat is an open-source Python framework for building real-time voice and multimodal conversational agents. From version 0.0.90 to before version 1.2.0, a path traversal vulnerability exists in Pipecat's development runner (src/pipecat/runner/run.py). When the runner is started with the --folder flag, it exposes a GET /files/{filename:path} download endpoint. The filename path parameter is concatenated directly onto args.folder with no containment check. Starlette normalises literal ../ sequences in URLs, but %2F-encoded slashes bypass this normalisation: the path parameter is URL-decoded after routing, so ../%2F..%2Fetc%2Fpasswd resolves to a path two levels above args.folder. An attacker with network access to the runner can read any file the pipecat process has permission to access - including SSH private keys, credentials, and system files - with a single unauthenticated HTTP request. This issue has been patched in version 1.2.0.	2026-06-09	7.5	CVE-2026-44716
plasmaticmedia--Recover Exit For WooCommerce	The Recover Exit For WooCommerce plugin for WordPress is vulnerable to Local File Inclusion in all versions up to and including 1.0.3. This is due to insufficient validation and sanitization of the user-controlled `tpf` POST parameter before it is used in an `include()` path in the `recover_exit()` function. This makes it possible for unauthenticated attackers to perform path traversal and include unintended local PHP files, which can lead to sensitive information exposure and, in certain deployment chains, code execution.	2026-06-09	8.1	CVE-2026-9662
QuanticaLabs--Car Park Booking System	WordPress Car Park Booking Plugin version 13 October 17 contains a time-based SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the space_id parameter. Attackers can send GET requests to the booking-page endpoint with malicious space_id values using AND SLEEP() payloads to extract sensitive database information.	2026-06-09	8.2	CVE-2017-20243
Rapid7--Velociraptor	A YAML injection vulnerability exists in the Windows.Collectors.Remapping artifact of Rapid7 Velociraptor before version 0.76.6. The hostname field in client_info.json inside a collection ZIP is inserted into a YAML template via Go's text/template without escaping. An attacker providing a crafted collection ZIP can leverage literal double quotes and newlines in the hostname to break out of the YAML quoted string and inject a new mount remapping entry. When an analyst applies the generated remapping file with --remap, arbitrary VQL executes on their machine with NullACLManager (all permissions granted, unsandboxed).	2026-06-09	7.8	CVE-2026-8795
raszi--node-tmp	tmp is a temporary file and directory creator for node.js. In version 0.2.6, the _assertPath guard added to tmp rejects only string values that contain the substring ... It is bypassed when prefix, postfix, or template is supplied as a non-string value (Array, Buffer, or any object) whose includes('.') returns falsy but whose stringification still contains ../. The value flows through Array.prototype.join/String coercion inside _generateTmpName and path.join(tmpDir, opts.dir, name), producing a final path that escapes tmpdir and creates a file or directory at an attacker-controlled location with the host process's privileges. This affects any application that forwards untrusted request data (a common pattern is JSON body fields or qs-parsed bracket-array query strings such as ?prefix[]=...) into tmp.file, tmp.fileSync, tmp.dir, tmp.dirSync, tmp.tmpName, or tmp.tmpNameSync without explicit type coercion. This vulnerability is fixed in 0.2.7.	2026-06-11	8.2	CVE-2026-49982
Red Hat Inc--Migration-Agent	A flaw was found in assisted-migration-agent. The application hardcodes insecure Transport Layer Security (TLS) connections when communicating with vCenter. This vulnerability allows a Man-in-the-Middle (MITM) attacker to intercept and harvest vCenter administrator credentials. This can lead to unauthorized access to vCenter.	2026-06-10	9.3	CVE-2026-53475
Red Hat Inc--Migration-Agent	A flaw was found in assisted-migration-agent. An unauthenticated attacker, located on the same local area network (LAN), can exploit a path traversal vulnerability. By crafting a specially designed gzipped tarball, the attacker can bypass security checks and write arbitrary files to the system.	2026-06-10	9.6	CVE-2026-53476

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This could ultimately lead to the execution of unauthorized code on the appliance.			
Red Hat Inc-- Migration-Planner	A flaw was found in migration-planner. An authenticated user can exploit this vulnerability by sending a DELETE request to the /api/v1/sources route, which lacks proper authorization and filtering. This allows for the destruction of all customer data, including sources, agents, and assessments, leading to a critical loss of availability and integrity across the entire SaaS platform.	2026-06-10	9.1	CVE-2026-53469
Red Hat Inc-- Migration-Planner	A flaw was found in migration-planner. An authenticated attacker could exploit an improper access control vulnerability in the /api/v1/sources/{id}/image-url` endpoint. This flaw allows the attacker to bypass an ownership check and obtain presigned S3 URLs for Open Virtual Appliance (OVA) images belonging to other users. Consequently, the attacker can download OVA images containing sensitive information, such as long-lived agent JSON Web Tokens (JWTs) and source configurations, potentially leading to unauthorized access and modification of the victim's source.	2026-06-10	9.6	CVE-2026-53470
Red Hat Inc-- Migration-Planner	A flaw was found in migration-planner. The agent-API middleware processes JSON Web Tokens (JWTs) for authentication, but its UpdateSourceInventory and UpdateAgentStatus handlers fail to validate the source_id claim within these tokens against the requested source ID. This oversight allows an authenticated attacker with a valid agent token to manipulate data across different tenants, leading to a complete collapse of tenant isolation. This could result in unauthorized overwriting of victim inventory, planting of malicious credential URLs, or corruption of migration assessments.	2026-06-10	9.6	CVE-2026-53471
Red Hat Inc-- Migration-Planner	A flaw was found in migration-planner. A remote authenticated attacker could exploit this vulnerability by uploading a specially crafted RVTools .xlsx file. Due to improper input sanitization, malicious SQL embedded within a spreadsheet cell is executed when cluster names are processed. This SQL Injection allows for arbitrary file reading on the system, potentially exposing sensitive information such as Kubernetes service account tokens and other credentials, which could lead to a full compromise of the SaaS environment.	2026-06-10	9.6	CVE-2026-53474
Red Hat Inc-- Migration-Planner-ui-app	A flaw was found in migration-planner-ui-app. An attacker can register a malicious discovery agent with a specially crafted credentialUrl containing JavaScript code. When an organizational user clicks this link in the user interface, the embedded malicious code executes within the user's browser session. This cross-site scripting (XSS) vulnerability allows the attacker to compromise the victim's Red Hat Single Sign-On (SSO) session, potentially leading to unauthorized cross-tenant data access and API actions.	2026-06-10	7.3	CVE-2026-53473
Red Hat--Red Hat Build of Keycloak	A flaw was found in Keycloak. A limited administrator can exploit an improper access control vulnerability in the POST /admin/realms/{realm}/partialImport endpoint. This allows them to bypass Fine-Grained Admin Permissions (FGAP) and escalate their privileges to a full realm administrator by importing users with realm-admin role mappings.	2026-06-08	7.2	CVE-2026-11577
Red Hat--Red Hat Directory Server 11	An integer overflow flaw was found in the SASL I/O layer of 389 Directory Server (389-ds-base). In sasl_io_start_packet(), adding sizeof(uint32_t) to a crafted SASL packet length prefix of 0xFFFFFFFFC causes unsigned wraparound to zero, bypassing the nsslapd-maxsaslioseize limit and leading to a heap buffer overflow of up to approximately 2 megabytes of attacker-controlled data. After a successful SASL bind with integrity protection (SSF > 0), a remote attacker can cause a Denial of Service (DoS) or achieve Remote Code Execution (RCE). In FreeIPA and Red Hat Identity Management deployments, any domain user with a valid Kerberos ticket, enrolled host, or service account can trigger this vulnerability over the	2026-06-11	7.6	CVE-2026-11774

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	network. This flaw is independent of CVE-2025-14905, which patched schema.c only and did not modify sasl_io.c.			
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in dracut. A remote attacker on the adjacent network can exploit this vulnerability by providing specially crafted DHCP (Dynamic Host Configuration Protocol) options, such as a malicious hostname, to a system using dracut's legacy DHCP path. These options are improperly handled and written into temporary shell scripts without proper escaping, leading to command injection. This allows the attacker to achieve root code execution within the initramfs, potentially compromising the system's boot and network behavior.	2026-06-10	8.8	CVE-2026-6893
Red Hat--Red Hat Enterprise Linux 10	A local privilege escalation vulnerability was found in the ansible.posix authorized_key module. The module's keyfile() function uses os.chown() instead of os.lchown() and opens files without O_NOFOLLOW when managing SSH authorized keys. An unprivileged local user can pre-stage symbolic links in their ~/.ssh directory to redirect file ownership changes to arbitrary system paths when an operator runs the authorized_key task as root, leading to local privilege escalation.	2026-06-10	7.3	CVE-2026-11837
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in Samba's WINS server component when running as an Active Directory Domain Controller. The WINS protocol handlers for certain request types did not properly validate incoming packets, allowing an unauthenticated remote attacker to trigger a NULL pointer dereference and crash the WINS service using specially crafted UDP packets.	2026-06-08	7.5	CVE-2026-3238
Red Hat--Red Hat Enterprise Linux 6	A time-of-check time-of-use (TOCTOU) race condition was found in the abrt-dbus D-Bus service's SetElement method. Between dump directory creation and post-create event execution, any local user can call SetElement to write arbitrary text files into the root-owned dump directory, bypassing package validation and allowing crashes of unpackaged binaries to survive post-create processing.	2026-06-13	7.8	CVE-2026-54228
Red Hat--Red Hat Enterprise Linux 6	A race condition was found in the abrt-dbus D-Bus service's ChownProblemDir method. ChownProblemDir opens the dump directory with DD_OPEN_READONLY and calls dd_chown to change ownership of all files to the caller's uid, succeeding even while post-create event handlers hold a write lock. This allows an attacker to gain filesystem-level control of the dump directory while privileged event scripts are still running.	2026-06-13	7	CVE-2026-54229
Red Hat--Red Hat Enterprise Linux 6	A symlink following vulnerability was found in the ABRT post-create event handler scripts in libreport. Event scripts write output files using shell redirections without the O_NOFOLLOW flag. If the target file is replaced with a symlink, the shell process running as root follows the symlink and writes content to the symlink target, allowing arbitrary file overwrites on the system.	2026-06-13	7	CVE-2026-54230
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, PUT /smon/check (app/routes/smon/routes.py:117-138) gates only on roxywi_common.check_user_group_for_flask() - which validates that the caller has some group, not that the target check_id belongs to it. The downstream SQL update functions update_smon, update_smonHttp, update_smonTcp, update_smonPing, update_smonDns (app/modules/db/smon.py:515-562) all execute WHERE smon_id = ? with no user_group filter. The DELETE path is correctly filtered (app/modules/db/smon.py:319-327 does WHERE id = ? AND user_group = ?), demonstrating that the maintainers know the right pattern but did not apply it on UPDATE. Therefore any authenticated user can iterate over smon_id values and silently rewrite any other tenant's HTTP / TCP / Ping / DNS monitoring check. At time of publication, there are no publicly available patches.	2026-06-10	9.1	CVE-2026-45550
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, the install blueprint declares only bp.before_request @jwt_required() (app/routes/install/routes.py:36-39). The individual endpoints	2026-06-10	9.9	CVE-2026-45552

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	install_exporter, install_waf, install_geoip, check_geoip, get_exporter_version, and get_task_status are not wrapped in page_for_admin and do not call roxywi_common.is_user_has_access_to_its_group(server_ip) or check_is_server_in_group(server_ip). Only the GET index page (install_monitoring) gates on roxywi_auth.page_for_admin(level=2). Because the missing decorators omit both role and group checks, any logged-in user - including the default guest role 4 - can install/reconfigure exporters, WAF, and GeoIP databases on every server in the Roxy-WI database, regardless of tenant ownership. The Ansible playbooks run with the per-server SSH credential stored in Roxy-WI, which the credentials' rightful owner (a different tenant) has provisioned with sudo rights for the management workflow. At time of publication, there are no publicly available patches.			
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, POST /waf/<service>/<server_ip>/rule/<rule_id>/save accepts a config_file_name form field that is passed straight through to config_mod.master_slave_upload_and_restart(...) as the destination path. The validation chain (_replace_config_path_to_correct ' check_is_conf) only requires the path to contain a hard-coded service substring (nginx/haproxy/apache2/httpd/keepalived) and the substring conf or cfg, and to not contain ... The encoded-slash substitution 92 ' / is applied before the substring check, so the attacker can build any absolute path anywhere on the LB filesystem as long as it satisfies those substring constraints. The body of the WAF rule (config form field) is written verbatim to that path. By choosing a filename like 92etc92cron.d92nginx_cfg_evil (resolving to /etc/cron.d/nginx_cfg_evil), an attacker drops a cron entry on the load balancer with attacker-controlled content. Cron parses the file on its next scan, executing the embedded job as root - full RCE on every load balancer the caller's group manages. At time of publication, there are no publicly available patches.	2026-06-10	9.9	CVE-2026-45556
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, the HAProxy section-save endpoints (POST /api/service/haproxy/<server_id>/section/<section_type> and the PUT /global / defaults variants) accept a JSON option field that is not validated, not escaped, and is rendered verbatim into the generated HAProxy configuration via the section.j2, global.j2, and defaults.j2 Ansible templates. Because Roxy-WI then pushes the generated config to the load balancer and runs systemctl reload haproxy, an authenticated user with role ' 3 (user) can inject arbitrary HAProxy directives into the config that runs on every load balancer their group manages - including option external-check + external-check command /bin/bash -c ' ', which gives remote code execution on the load balancer as the haproxy user on every health-check tick. At time of publication, there are no publicly available patches.	2026-06-10	9.9	CVE-2026-45558
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, agent_action (app/routes/smon/agent_routes.py:166-179) has decorators @bp.post('/agent/action/<action>') and @jwt_required() only - no role check, no group ownership check on the server_ip form field. Any authenticated user, including role 4 (guest), can start, stop, or restart the roxy-wi-smon-agent systemd unit on any server they can name. Roxy-WI executes the systemd action over its own SSH credentials (passwordless sudo), so the action runs as root on the target. At time of publication, there are no publicly available patches.	2026-06-10	8.5	CVE-2026-45549
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, POST	2026-06-10	8.8	CVE-2026-45564

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	/config/versions/<service>/<server_ip>/<configver>/save interpolates the URL-path configver parameter directly into a config-version path that ends up at os.system(f"dos2unix -q {cfg}"). configver is not run through EscapedString (Pydantic doesn't validate path segments declared as str) and the surrounding .. block is the broken tuple-membership patch from GHSA-vapt-004. An authenticated user with role <= 3 ("user") therefore reaches a bin/sh -c command-injection sink. At time of publication, there are no publicly available patches.			
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, EscapedString (app/modules/roxywi/class_models.py:16-30) is the centralised Pydantic validator used on dozens of fields including SSH credential name, username, description, etc. Its if/elif/elif/else flow returns the metacharacter-stripped value without also enforcing the .. block. An attacker who appends a single ;, &, , \$, or backtick to a .. payload routes the value through the strip arm, where .. survives unblocked and the result is not shlex.quote()'d either. At time of publication, there are no publicly available patches.	2026-06-10	8.1	CVE-2026-45565
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, there is an authentication bypass vulnerability via 'api' substring in URL + unauthenticated /api/gpt. At time of publication, there are no publicly available patches.	2026-06-10	8.3	CVE-2026-45567
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, ommit d4d10006 ("Expand validation to block .. in config_file_name and configver for improved security") added a line in app/modules/config/config.py:462. This is tuple-membership, not substring containment - '..' in (a, b, c) evaluates to True only if any of a, b, c is equal to the literal string '..'. For any realistic path-traversal payload (../etc/passwd, ../../etc/passwd, etc.) the check returns False and the patch silently lets the payload through. At time of publication, there are no publicly available patches.	2026-06-10	8.1	CVE-2026-45569
Ruijie--EG105G-P	A security flaw has been discovered in Ruijie EG105G-P 2.340. The impacted element is the function nslookup of the file /cgi-bin/luci/api/diagnose of the component JSON-RPC Diagnose Endpoint. Performing a manipulation of the argument params.target results in command injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-14	7.2	CVE-2026-12197
sahlberg--libnfs	libnfs through 6.0.2 before 55c18ea does not validate a string size, leading to an integer overflow during a connection to a crafted NFS server. This occurs in libnfs_zdr_string in lib/libnfs-zdr.c.	2026-06-10	7.1	CVE-2026-53689
SAP_SE--SAP NetWeaver Application Server Java (Web Container)	SAP NetWeaver Application Server Java (Web Container) allows an unauthenticated attacker to craft a malicious HTTP logon request that manipulates file inclusion parameters, enabling path traversal and processing of the included file. Processing the included file could allow the attacker to view or modify sensitive information or render any part of the local system unavailable.	2026-06-09	9	CVE-2026-40128
SAP_SE--SAP NetWeaver AS ABAP and ABAP Platform	Due to improper RFC protocol validation in the SAP Kernel used by the Application Server ABAP of SAP NetWeaver and ABAP Platform, an unauthenticated attacker can send a crafted RFC request that exploits logical errors in memory management, leading to memory corruption. This could lead to a high impact on the confidentiality, integrity, and availability of the application.	2026-06-09	9.8	CVE-2026-27671
SAP_SE--SAP NetWeaver AS ABAP and ABAP Platform	SAP NetWeaver Application Server ABAP and ABAP Platform allows an authenticated attacker with normal privileges to obtain a valid signed message and send modified signed XML documents to the verifier. This may result in acceptance of tampered identity information leading to unauthorized access to sensitive user data and potential disruption of	2026-06-09	9.9	CVE-2026-44748

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	normal system usage. This causes a high impact on confidentiality, integrity and availability of the application.			
SAP_SE--SAP NetWeaver AS ABAP and ABAP Platform	Application server ABAP does not perform necessary authorization checks for an authenticated user allowing an attacker to execute a report generation command which could overwrite information belonging to another user, resulting in escalation of privileges. This has high impact on integrity with low impact on availability and no impact on confidentiality of the application.	2026-06-09	7.1	CVE-2026-44751
Siemens--SIMATIC WinCC Unified PC Runtime V16	A vulnerability has been identified in SIMATIC WinCC Unified PC Runtime V16 (All versions), SIMATIC WinCC Unified PC Runtime V17 (All versions), SIMATIC WinCC Unified PC Runtime V18 (All versions), SIMATIC WinCC Unified PC Runtime V19 (All versions), SIMATIC WinCC Unified PC Runtime V20 (All versions), SIMATIC WinCC Unified PC Runtime V21 (All versions < V21 Update 2). Insufficient protection of key material in WinCC Certificate Manager that could allow an attacker to extract sensitive information.	2026-06-09	7.1	CVE-2026-24349
Siemens--SINEC INS	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 6). The application does not properly sanitize user input in the /api/sftp/uploadFiles endpoint, allowing the injection of shell command payloads via crafted directory names. These payloads are stored and executed when directory listings are retrieved. This could allow an authenticated remote attacker to execute arbitrary commands on the underlying operating system with the privileges of the affected service user (sinecins).	2026-06-09	8.8	CVE-2026-46746
Siemens--SINEC INS	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 6). The affected system includes a binary that is configured with the cap_dac_override capability. This capability allows the process to bypass file system permission checks, resulting in unrestricted file system access. This could allow a local attacker to escalate privileges leading to arbitrary file modification and gaining root privileges on the system.	2026-06-09	8.8	CVE-2026-46748
Siemens--SINEC INS	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 6). The affected application uses a password hashing implementation with a static, hardcoded salt shared across all users and installations, and is configured with an insufficient number of iterations. This could allow an attacker to efficiently recover user passwords using brute-force or precomputed attacks, potentially resulting in unauthorized access.	2026-06-09	7.5	CVE-2026-46749
signalwire--freeswitch	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.1, esl_recv_event() parses Content-Length with atol() and passes the result straight to malloc(len + 1) with no sign or magnitude check. A malicious or man-in-the-middle ESL peer can send a frame with a negative Content-Length to corrupt the heap of, or crash, any process linked against libesl, before the client has authenticated to that peer. This issue has been patched in version 1.11.1.	2026-06-09	9.1	CVE-2026-49840
signalwire--freeswitch	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.1, the mod_verto HTTP request handler allocates a fixed 2 MiB buffer for a POST application/x-www-form-urlencoded body but accepts Content-Length up to just under 10 MiB. The body-read loop is bounded by Content-Length rather than the buffer size, producing an attacker-controlled heap overflow of up to ~8 MiB -- before the HTTP basic-auth check runs. This issue has been patched in version 1.11.1.	2026-06-09	9.8	CVE-2026-49841
signalwire--freeswitch	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.0, FreeSWITCH's bundled XML parser expands nested <!ENTITY> declarations without a depth or count bound, so a small DTD can describe	2026-06-09	7.5	CVE-2026-45771

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a body that expands exponentially ("billion laughs"). The PIDF body of a SIP PUBLISH is fed to this parser before any digest check, letting an unauthenticated network attacker force unbounded CPU and memory consumption with a single request. This issue has been patched in version 1.11.0.			
signalwire-- freeswitch	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.0, a STUN packet whose declared attribute length is shorter than the structure the parser casts to causes the parser to read and write past the end of the attribute, producing an out-of-bounds memory access on the per-leg media buffer. This issue has been patched in version 1.11.0.	2026-06-09	7.5	CVE-2026-49475
signalwire-- freeswitch	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.1, mod_verto's WebSocket frame loop intercepts a #-prefixed speed-test protocol (#SPU / #SPB / #SPE) before any authentication check. The declared payload size in #SPU was parsed with atoi() and only rejected non-positive values, so an unauthenticated peer could request up to INT_MAX bytes. The server then wrote roughly size * 10 bytes back during the download phase, on the order of 20 GB per request, yielding strong outbound bandwidth amplification from a short request. This issue has been patched in version 1.11.1.	2026-06-09	7.5	CVE-2026-49842
signalwire-- freeswitch	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.1, a single unauthenticated WebSocket frame containing a deeply nested JSON document crashes the FreeSWITCH process via stack overflow, terminating all calls and sessions on the host. The recursion drives the worker thread's stack pointer into the stack guard page, raising SIGSEGV from the kernel before any usable write primitive develops. This issue has been patched in version 1.11.1.	2026-06-09	7.5	CVE-2026-49847
SimpleHelp-- SimpleHelp	SimpleHelp versions 5.5.15 and prior and 6.0 pre-release versions contain an authentication bypass vulnerability in the OIDC authentication flow. When OIDC authentication is configured, identity tokens submitted during login are accepted without verifying their cryptographic signature. In a vulnerable configuration, a remote, unauthenticated attacker can submit a forged token containing arbitrary identity claims to obtain a fully authenticated technician session. In some configurations, this may also allow bypass of multi-factor authentication. No user interaction is required.	2026-06-12	10	CVE-2026-48558
simplesamlphp-- simplesamlphp- module- casserver	SimpleSAMLphp-casserver is a CAS 1.0 and 2.0 compliant CAS server in the form of a SimpleSAMLphp module. Prior to version 7.0.3, simplesamlphp-module-casserver builds file paths for the file-based CAS ticket store by directly concatenating the configured ticket directory with an attacker-controlled ticket identifier. Public CAS validation/proxy endpoints pass attacker-controlled ticket / pgt query parameters into this store. In deployments using FileSystemTicketStore, a remote attacker can use path traversal sequences such as ../target.serialized to make the CAS server read and unserialize files outside the ticket directory. In the CAS 1.0 validation flow, the same attacker-selected path is also passed to deleteTicket() immediately after getTicket() returns, which can delete the target file when it is readable by the PHP process, deletable under the PHP process filesystem permissions, and unserializes to a value compatible with the ?array return type. This issue has been patched in version 7.0.3.	2026-06-09	8.6	CVE-2026-46491
sixstorage-- 6Storage Rentals	The 6Storage Rentals plugin for WordPress is vulnerable to Authorization Bypass Through User-Controlled Key in all versions up to and including 2.22.0 via the `userId` parameter of the `six_storage_get_user_info` and `six_storage_update_profile` AJAX actions. This is due to the	2026-06-09	7.5	CVE-2026-9185

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`six_storage_getUserInfo()` and `six_storage_updateProfile()` functions being registered on `wp_ajax_nopriv_*` hooks and accepting a tenant identifier directly from `\$_POST['userId']` without performing any ownership verification, session binding, or nonce validation to confirm the requester has a legitimate relationship to the supplied ID. This makes it possible for unauthenticated attackers to read and modify arbitrary tenants' profile data - including name, email address, phone number, physical address, and SSN - by supplying an enumerated `userId` value in a crafted request to either handler.			
Skilja GmbH-- Vinna Process Monitor	A Stored Cross-Site Scripting vulnerability in Vinna Process Monitor Version 4.0 Service Pack 1 (Build 63255) allows an authenticated remote attacker with low privileges to inject malicious JavaScript code into the application. This enables attackers to steal administrative access tokens and session credentials.	2026-06-09	8.7	CVE-2026-41031
Soagen Informatics Technologies Software and Consulting Inc.-- Apinizer	Improper neutralization of special elements used in an expression language statement ('expression language injection') vulnerability in Soagen Informatics Technologies Software and Consulting Inc. Apinizer allows Code Injection. This issue affects Apinizer: from 2026.04.0 before 2026.04.6.	2026-06-11	9.8	CVE-2026-11561
SolidInvoice-- SolidInvoice	SolidInvoice is an open-source invoicing platform. Prior to version 2.3.17, the company logo upload feature accepts any file type without validation. An authenticated administrator can upload an SVG file containing embedded JavaScript. This script is base64-encoded and injected unescaped into every page of the application, causing stored cross-site scripting (XSS) that executes in every authenticated user's browser. This issue has been patched in version 2.3.17.	2026-06-11	8.1	CVE-2026-46489
SolidInvoice-- SolidInvoice	SolidInvoice is an open-source invoicing platform. Prior to version 2.3.17, API tokens used to authenticate all REST API requests are stored as plaintext strings in the api_tokens database table. Any attacker who obtains read access to the database - through SQL injection, a leaked backup, a misconfigured replica, or insider access - immediately obtains all API credentials for every user with no further effort. This issue has been patched in version 2.3.17.	2026-06-11	8.1	CVE-2026-46622
Sonaar--Sonaar Music Plugin	WordPress Sonaar Music Plugin 4.7 contains a stored cross-site scripting vulnerability that allows unauthenticated attackers to inject malicious scripts through the comment functionality. Attackers can submit JavaScript payloads in the comment parameter to wp-comments-post.php which are stored and executed in the browsers of users viewing the affected playlist pages.	2026-06-08	7.2	CVE-2023-54351
SourceCodester-- Class and Exam Timetabling System	A vulnerability was found in SourceCodester Class and Exam Timetabling System 1.0. The impacted element is an unknown function of the file /index2.php. The manipulation of the argument Password results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	2026-06-08	7.3	CVE-2026-11471
SourceCodester-- Class and Exam Timetabling System	A vulnerability was determined in SourceCodester Class and Exam Timetabling System 1.0. This affects an unknown function of the file /index1.php. This manipulation of the argument Password causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2026-06-08	7.3	CVE-2026-11472
SourceCodester-- Class and Exam Timetabling System	A vulnerability was identified in SourceCodester Class and Exam Timetabling System 1.0. The impacted element is an unknown function of the file /archive5.php. The manipulation of the argument sy leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	2026-06-08	7.3	CVE-2026-11482
SourceCodester-- Class and Exam Timetabling System	A security flaw has been discovered in SourceCodester Class and Exam Timetabling System 1.0. This affects an unknown function of the file /archive4.php. The manipulation of the argument sy results in sql	2026-06-08	7.3	CVE-2026-11483

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.			
SourceCodester--Class and Exam Timetabling System	A weakness has been identified in SourceCodester Class and Exam Timetabling System 1.0. This impacts an unknown function of the file /archive3.php. This manipulation of the argument sy causes sql injection. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks.	2026-06-08	7.3	CVE-2026-11484
SourceCodester--Class and Exam Timetabling System	A security vulnerability has been detected in SourceCodester Class and Exam Timetabling System 1.0. Affected is an unknown function of the file /archive2.php. Such manipulation of the argument sy leads to sql injection. The attack may be launched remotely. The exploit has been disclosed publicly and may be used.	2026-06-08	7.3	CVE-2026-11485
SourceCodester--Class and Exam Timetabling System	A vulnerability was detected in SourceCodester Class and Exam Timetabling System 1.0. Affected by this vulnerability is an unknown functionality of the file /archive1.php. Performing a manipulation of the argument sy results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	2026-06-08	7.3	CVE-2026-11486
SourceCodester--Hospitals Patient Records Management System	A security flaw has been discovered in SourceCodester Hospitals Patient Records Management System 1.0. This issue affects some unknown processing of the file /classes/Master.php?f=save_patient. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	2026-06-08	7.3	CVE-2026-11501
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.2.4 and 10.0.7, and Splunk Cloud Platform versions below 10.4.2604.3 and 10.2.2510.14, an unauthenticated user could create or truncate arbitrary files through a PostgreSQL sidecar service endpoint. The vulnerability exists because the PostgreSQL sidecar service endpoint lacks authentication controls, allowing any network-reachable user to invoke file operations without credentials.	2026-06-10	9.8	CVE-2026-20253
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.2.4, 10.0.7, 9.4.12, and 9.3.13, Splunk Cloud Platform versions below 10.3.2512.12, 10.2.2510.14, 10.1.2507.22, and 9.3.2411.132, and Splunk Secure Gateway versions below 3.10.6, 3.9.20, and 3.8.67, a low-privileged user that does not hold the 'admin' or 'power' Splunk roles could perform a Remote Code Execution (RCE) through the Splunk Secure Gateway app. The Remote Code Execution is possible because of unsafe deserialization of App Key Value Store (KV Store) data through the 'jsonpickle' Python library, which reconstructs arbitrary Python objects from specially crafted JavaScript Object Notation (JSON) without adequate validation.	2026-06-10	8.8	CVE-2026-20251
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.2.4, 10.0.7, 9.4.12, and 9.3.13, and Splunk Cloud Platform versions below 10.4.2604.3, 10.3.2512.12, 10.2.2510.14, 10.1.2507.22, and 9.3.2411.132, a low-privileged user that does not hold the "admin" or "power" Splunk roles could send server-side requests to arbitrary internal destinations through the Dashboard Studio PDF export feature. The vulnerability exists because the trusted-domain validation uses a prefix match that can be bypassed with attacker-controlled subdomains (for example, docs.splunk.com.evil.com), and because the PDF export service follows HTTP redirects automatically without re-validating each redirect target against the allowlist.	2026-06-10	7.6	CVE-2026-20252
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.2.4, 10.0.7, 9.4.12, and 9.3.13, and Splunk Cloud Platform versions below 10.3.2512.11, 10.2.2510.15, 10.1.2507.23, and 9.3.2411.132, a low-privileged user that does not hold the "admin" or "power" Splunk roles could store a malicious script in a classic dashboard HTML panel, causing unauthorized JavaScript code to execute in the browser of another user. The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. The low-privileged user should not be able to exploit the vulnerability at will.	2026-06-10	7.1	CVE-2026-20258

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Spring--Micrometer	In Micrometer, it is possible for a user to provide specially crafted gRPC requests that may cause a denial-of-service (DoS) condition. Affected versions: Micrometer 1.16.0 through 1.16.5; 1.15.0 through 1.15.11.	2026-06-09	7.5	CVE-2026-40983
Spring--Micrometer	In Micrometer, it is possible for a user to provide specially crafted HTTP requests that may cause a denial-of-service (DoS) condition. Affected versions: micrometer-core 1.16.0 through 1.16.5; 1.15.0 through 1.15.11; 1.14.0 through 1.14.15; 1.13.0 through 1.13.18; 1.9.0 through 1.9.17. micrometer-jetty11 1.16.0 through 1.16.5; 1.15.0 through 1.15.11; 1.14.0 through 1.14.15; 1.13.0 through 1.13.18. micrometer-jetty12 1.16.0 through 1.16.5; 1.15.0 through 1.15.11; 1.14.0 through 1.14.15; 1.13.0 through 1.13.18.	2026-06-09	7.5	CVE-2026-40984
Spring--Spring Data Commons	Spring Data Commons applications may be vulnerable to denial of service through resource exhaustion when attacker-controlled property path strings are passed to MappingContext property path resolution. Affected versions: Spring Data Commons 4.0.0 through 4.0.5; 3.5.0 through 3.5.11; 3.4.0 through 3.4.14.	2026-06-09	7.5	CVE-2026-41695
Spring--Spring Data Commons	Spring Data's internal property-lookup cache accepts and permanently retains attacker-supplied strings as cache keys, allowing heap exhaustion through repeated requests. Affected versions: Spring Data Commons 2.7.0 through 2.7.19; 3.3.0 through 3.3.16; 3.4.0 through 3.4.14; 3.5.0 through 3.5.11; 4.0.0 through 4.0.5.	2026-06-09	7.5	CVE-2026-41716
Spring--Spring Data MongoDB	Spring Data MongoDB contains a SpEL (Spring Expression Language) expression injection vulnerability. The issue occurs during parameter binding when a user-defined repository query method is annotated with @Query and utilizes a capture-all placeholder. Affected versions: Spring Data MongoDB 5.0.0 through 5.0.5; 4.5.0 through 4.5.11; 4.4.0 through 4.4.14; 4.3.0 through 4.3.16; 4.2.0 through 4.2.15; 4.1.0 through 4.1.14; 4.0.0 through 4.0.15; 3.4.0 through 3.4.19.	2026-06-09	8.1	CVE-2026-41717
Spring--Spring Data REST	Spring Data REST is vulnerable to SpEL expression injection through map-typed properties when processing JSON Patch (application/json-patch+json) requests. When a persistent entity exposes a Map-typed property, the JSON Pointer path segment used as the map key is embedded directly into a SpEL expression without sanitization or validation. Affected versions: Spring Data REST 3.7.0 through 3.7.19; 4.3.0 through 4.3.16; 4.4.0 through 4.4.14; 4.5.0 through 4.5.11; 5.0.0 through 5.0.5.	2026-06-09	8.1	CVE-2026-41729
Spring--Spring Data REST	Spring Data REST's JSON Patch (application/json-patch+json) implementation does not apply the write-access filter to intermediate path segments when resolving a multi-segment JSON Pointer. Affected versions: Spring Data REST 3.7.0 through 3.7.19; 4.3.0 through 4.3.16; 4.4.0 through 4.4.14; 4.5.0 through 4.5.11; 5.0.0 through 5.0.5.	2026-06-09	7.5	CVE-2026-41728
Spring--Spring for Apache Kafka	JsonKafkaHeaderMapper and the deprecated DefaultKafkaHeaderMapper matched type headers against trusted packages using a prefix check, meaning that trusting any package implicitly trusted all of its subpackages. Combined with Jackson's default bean deserialization, a producer could supply crafted header values that caused the consumer to deserialize arbitrary JDK types. Affected versions: Spring for Apache Kafka 4.0.0 through 4.0.5; 3.3.0 through 3.3.15; 3.2.0 through 3.2.13; 2.9.0 through 2.9.13; 2.8.0 through 2.8.11.	2026-06-09	8.1	CVE-2026-41731
Spring--Spring for Apache Pulsar	JsonPulsarHeaderMapper matched type headers against trusted packages using a prefix check, meaning that trusting any package implicitly trusted all of its subpackages. Additionally, an empty trusted-packages configuration fell back to trusting all packages rather than applying a safe default allow-list. Affected versions: Spring for Apache Pulsar 2.0.0 through 2.0.5; 1.2.0 through 1.2.17; 1.1.0 through 1.1.17.	2026-06-09	8.1	CVE-2026-41732
Spring--Spring for GraphQL	Spring for GraphQL applications are vulnerable to Unsafe Deserialization when processing paginated GraphQL queries. An attacker can craft a malicious GraphQL request that can lead to Remote Code Execution when the application exposes a paginated (Connection) field and the classpath	2026-06-11	8.1	CVE-2026-41699

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	contains specific classes that can be leveraged during deserialization. Affected versions: Spring for GraphQL 2.0.0 through 2.0.3; 1.4.0 through 1.4.5; 1.3.0 through 1.3.8.			
Spring--Spring for GraphQL	Spring for GraphQL applications that have enabled the WebSocket transport are vulnerable to Cross-Site WebSocket Hijacking. An attacker can trick an authenticated user into visiting a malicious page, allowing the attacker to execute arbitrary GraphQL operations with the victim's credentials. Affected versions: Spring for GraphQL 2.0.0 through 2.0.3; 1.4.0 through 1.4.5; 1.3.0 through 1.3.8; 1.0.0 through 1.0.6.	2026-06-11	8.1	CVE-2026-41700
Spring--Spring for GraphQL	The Spring GraphQL annotation detection mechanism for @Controller data fetchers may not correctly resolve annotations on methods within type hierarchies. This can be an issue if such annotations are used for authorization decisions. When all conditions are met, security annotations can be ignored at runtime. Affected versions: Spring for GraphQL 2.0.0 through 2.0.3; 1.4.0 through 1.4.5; 1.3.0 through 1.3.8; 1.0.0 through 1.0.6.	2026-06-11	7.5	CVE-2026-41856
Spring--Spring Framework	In an untrusted JMS environment, org.springframework.jms.support.converter.MappingJackson2MessageConverter and org.springframework.jms.support.converter.JacksonJsonMessageConverter allow arbitrary class instantiation, which can lead to unauthorized actions via gadget class deserialization. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	8.1	CVE-2026-41855
Spring--Spring Framework	Spring MVC and WebFlux applications are vulnerable to Denial of Service (DoS) attacks when resolving static resources. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	7.5	CVE-2026-41842
Spring--Spring Framework	Due to incorrect escaping, the use of JavaScriptUtils.javaScriptEscape() may lead to JavaScript code injection in the browser, potentially resulting in a cross-site scripting (XSS) vulnerability. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	7.1	CVE-2026-41845
Spring--Spring Framework	An integer overflow vulnerability exists in the evaluation logic of the Spring Expression Language (SpEL). An attacker can exploit this by supplying a specially crafted SpEL expression that triggers excessive resource consumption, resulting in a Denial of Service (DoS). Affected versions: Spring Framework 5.3.0 through 5.3.48.	2026-06-09	7.5	CVE-2026-41849
Spring--Spring Framework	Applications that evaluate user-supplied Spring Expression Language (SpEL) expressions are vulnerable to an Algorithmic Denial of Service (DoS). By providing a specially crafted expression, an attacker can trigger excessive resource consumption during evaluation, leading to application degradation or unavailability. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	7.5	CVE-2026-41850
Spring--Spring HATEOAS	Spring HATEOAS's internal PropertyUtils.createObjectFromProperties method, used by the Collection+JSON and UBER media type deserializers, performs bean property binding via reflection without consulting Jackson access-control annotations. Affected versions: Spring HATEOAS 1.5.0 through 1.5.6; 2.3.0 through 2.3.4; 2.4.0 through 2.4.1; 2.5.0 through 2.5.2; 3.0.0 through 3.0.3.	2026-06-09	7.5	CVE-2026-41006
Spring--Spring HATEOAS	Spring HATEOAS maintains an unbounded static cache of StringLinkRelation instances keyed on attacker-supplied strings. Affected versions: Spring HATEOAS 1.5.0 through 1.5.6; 2.3.0 through 2.3.4; 2.4.0 through 2.4.1; 2.5.0 through 2.5.2; 3.0.0 through 3.0.3.	2026-06-09	7.5	CVE-2026-41007
Spring--Spring Integration	A malicious or compromised FTP/SFTP/SMB server can write arbitrary files anywhere on the client filesystem (outside the configured local-directory) with attacker-controlled content. Affected versions: Spring Integration 7.0.0 through 7.0.4; 6.5.0 through 6.5.8; 6.4.0 through 6.4.11; 6.3.0 through 6.3.14; 5.5.0 through 5.5.20.	2026-06-11	7.1	CVE-2026-40987

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Spring--Spring LDAP	Spring LDAP's DirContextAuthenticationStrategy implementations do not reject a bind request where a non-empty username is paired with an empty or null password. Affected versions: Spring LDAP 2.4.0 through 2.4.4; 3.2.0 through 3.2.17; 3.3.0 through 3.3.7; 4.0.0 through 4.0.3.	2026-06-09	7.4	CVE-2026-41720
Spring--Spring Security	An application using spring-security-saml2-service-provider and the REDIRECT binding for SAML 2.0 Login or Logout may be vulnerable to a denial of service by way of an unbounded writer that inflates the compressed SAML payload into memory. Affected versions: Spring Security 5.7.0 through 5.7.23; 5.8.0 through 5.8.25; 6.3.0 through 6.3.16; 6.4.0 through 6.4.16; 6.5.0 through 6.5.10; 7.0.0 through 7.0.5.	2026-06-09	7.5	CVE-2026-40988
Spring--Spring Security	An attacker with write permissions to the database table managed by JdbcAssertingPartyMetadataRepository (saml2_asserting_party_metadata) may be able to store malicious serialized payloads in the columns containing the collection of verification or encryption credentials (verification_credentials and encryption_credentials, respectively). Affected versions: Spring Security 7.0.0 through 7.0.5.	2026-06-09	7.3	CVE-2026-40993
Spring--Spring Security	An attacker able to influence values in RelyingPartyRegistration may be able to run arbitrary code on HTML forms generated by Spring Security filters. Affected versions: Spring Security 5.7.0 through 5.7.23; 5.8.0 through 5.8.25; 6.3.0 through 6.3.16; 6.4.0 through 6.4.16; 6.5.0 through 6.5.10; 7.0.0 through 7.0.5.	2026-06-09	7.6	CVE-2026-41003
Spring--Spring Web Services	Wss4jSecurityInterceptor initialized its BSP (WS-I Basic Security Profile) compliance flag so that inbound validation disabled WSS4J BSP enforcement on RequestData. Services that validate WS-Security on the network could therefore accept messages that violate BSP rules, weakening protocol-level checks. Affected versions: Spring Web Services 5.0.0 through 5.0.1; 4.1.0 through 4.1.3; 4.0.0 through 4.0.18; 3.1.0 through 3.1.8.	2026-06-11	8.2	CVE-2026-40994
Spring--Spring Web Services	Jaxp13XPathTemplate evaluated XPath expressions for StreamSource and SAXSource inputs using a code path that parsed attacker-controlled XML with the JDK's default DocumentBuilderFactory behavior instead of Spring's hardened parser configuration. Applications that evaluate XPath against untrusted XML payloads could therefore be exposed to XML External Entity (XXE) style attacks. Affected versions: Spring Web Services 5.0.0 through 5.0.1; 4.1.0 through 4.1.3; 4.0.0 through 4.0.18; 3.1.0 through 3.1.8.	2026-06-11	8.2	CVE-2026-40998
Spring--Spring Web Services	When WS-Addressing is used with non-anonymous ReplyTo or FaultTo addresses, Spring WS may initiate outbound connections through configured WebServiceMessageSender instances to destinations taken directly from request headers without verifying that those destinations are safe to connect to. Affected versions: Spring Web Services 5.0.0 through 5.0.1; 4.1.0 through 4.1.3; 4.0.0 through 4.0.18; 3.1.0 through 3.1.8.	2026-06-11	8.6	CVE-2026-40999
sqlfluff--sqlfluff	SQLFluff is a modular SQL linter and auto-formatter with support for multiple dialects and templated code. Prior to version 4.1.0, in deployments where untrusted users can provide SQL queries to be linted, an untrusted user can submit a malicious query with deliberate excessive nesting to any application using the parser to trigger a Denial of Service through resource exhaustion. This issue has been patched in version 4.1.0.	2026-06-09	7.5	CVE-2026-46373
sqlfluff--sqlfluff	SQLFluff is a modular SQL linter and auto-formatter with support for multiple dialects and templated code. Prior to version 4.2.0, in deployments where untrusted users can provide SQL queries to be linted, an untrusted user can submit a malicious long query to any application using the parser to trigger a Denial of Service through resource exhaustion. This issue has been patched in version 4.2.0.	2026-06-09	7.5	CVE-2026-46374
SQLite--SQLite	SQLite before 3.53.2 contains memory corruption vulnerabilities in the FTS5 full-text search extension that allow attackers to cause process crashes, memory exhaustion, or arbitrary code execution by supplying a crafted database with malformed FTS5 page data. Attackers can trigger an out-of-bounds read in fts5LeafSeek() via an attacker-controlled loop bound	2026-06-09	7.8	CVE-2026-11822

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and a heap buffer overflow write in fts5ChunkIterate() through a crafted continuation page causing an integer underflow, exploitable when an FTS5 MATCH query is executed against the malicious database.			
SQLite--SQLite	SQLite before 3.53.2 contains a heap-based buffer overflow vulnerability in the FTS5 full-text search extension that allows attackers to cause a crash or execute arbitrary code by supplying a crafted database with malicious continuation page metadata specifying a szLeaf value smaller than 4. Attackers can trigger an integer underflow in fts5ChunkIterate() causing an inflated remaining byte count during FTS5 MATCH query processing, leading to a heap buffer overflow of attacker-controlled data in applications compiled with SQLITE_ENABLE_FTS5.	2026-06-09	7.8	CVE-2026-11824
STACKIT--IaaS API	STACKIT IaaS API contains a missing authorization check vulnerability that allows authenticated, low-privileged attackers to escalate privileges to full organization compromise by attaching arbitrary service accounts to virtual machines they control. Attackers can exploit the unvalidated PUT servers service-accounts endpoint to attach high-privileged service accounts and query the Instance Metadata Service to retrieve OAuth2 tokens, bypassing tenant boundaries and gaining unauthorized control over the entire organization environment.	2026-06-08	9.8	CVE-2026-39910
stefanbohacek--fediverse-embeds-wordpress-plugin	Fediverse Embeds embeds fediverse posts on WordPress sites. Prior to version 1.5.8, Fediverse Embeds registered an unauthenticated REST route ftf/media-proxy (includes/Media_Proxy.php) with permission_callback => __return_true that accepted a base64-encoded URL and forwarded it to wp_remote_get(\$url) without enforcing any allowlist. The plugin's source contained a comment block explicitly acknowledging that the request should be validated against allowed fediverse domains, but in 1.5.7 the validation only set a local \$can_download_media flag that was never read. The full response body was echoed back to the caller, so this was a full-read SSRF / open proxy reachable by any anonymous visitor. This issue has been patched in version 1.5.8.	2026-06-11	7.5	CVE-2026-46697
steipete--summarize	Summarize before 0.17.0 contains a server-side request forgery vulnerability that allows attackers who control a podcast RSS feed to direct the host to fetch transcript content from loopback addresses, link-local addresses, RFC 1918 private ranges, or other reserved destinations by supplying malicious podcast:transcript URL values. Attackers can bypass protections through DNS rebinding and redirect-based techniques, as redirect targets are not revalidated and hostnames are not resolved before request dispatch, exposing internal service responses through the summarization flow.	2026-06-11	7.4	CVE-2026-53782
stiofansisland--Events Calendar for GeoDirectory	The Events Calendar for GeoDirectory plugin for WordPress is vulnerable to Privilege Escalation in versions up to and including 2.3.28. This is due to the ajax_ayi_action() handler only applying strip_tags(esc_sql()) - with no allow-list - to the attacker-controlled \$_POST['type'] and \$_POST['postid'] values before forwarding them to update_ayi_data(), which calls update_user_meta(\$current_user->ID, \$rsvp_args['type'], \$posts). By passing type=wp_capabilities and postid=administrator, an attacker writes ['subscriber'=>true,'administrator'=>'administrator'] into their own wp_capabilities user meta; WP_User::get_role_caps() then treats the 'administrator' array key as an active role on the next request. This makes it possible for authenticated attackers, with Subscriber-level access and above, to elevate their privileges to Administrator.	2026-06-09	8.8	CVE-2026-11616
sveltejs--devalue	Svelte devalue is a JavaScript library that serializes values into strings when JSON.stringify isn't sufficient for the job. From version 5.6.3 to before version 5.8.1, devalue.parse could, due to quirks in some JavaScript engines, be convinced to allocate much more memory than was needed when deserializing sparse arrays, leading to excessive memory consumption. This issue has been patched in version 5.8.1.	2026-06-09	7.5	CVE-2026-42570
Systerel--S2OPC	Improper comparison with the certificates trusted list in S2OPC allows an attacker well-formed untrusted certificate to be considered trusted	2026-06-10	7.3	CVE-2026-9758

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tale--headplane	Headplane is a feature-complete Web UI for Headscale. Prior to versions 0.6.3 and 0.7.0-beta.3, Headplane was vulnerable to a path traversal / authorization bypass in the Headscale API client used by node and user rename operations. This issue has been patched in versions 0.6.3 and 0.7.0-beta.3.	2026-06-08	8.1	CVE-2026-46484
taosdata--TDengine	TDengine is an open source, time-series database optimized for Internet of Things devices. In versions 3.4.0.0 through 3.4.1.5, an unauthenticated remote attacker can crash the taosd server process by sending a single crafted RPC packet. No credentials or prior session state are required. Version 3.4.1.6 fixes the issue.	2026-06-10	7.5	CVE-2026-42542
Tenda--AC18	A vulnerability was found in Tenda AC18 15.03.05.05. The affected element is the function sub_45304 of the file /goform/getRebootStatus of the component Web Management Interface. The manipulation of the argument callback results in stack-based buffer overflow. The attack may be launched remotely. The exploit has been made public and could be used.	2026-06-08	8.8	CVE-2026-11528
Tenda--CX12L	A security vulnerability has been detected in Tenda CX12L 16.03.53.12. The affected element is the function form_fast_setting_wifi_set of the file /goform/fast_setting_wifi_set of the component Wi-Fi Configuration Endpoint. Such manipulation of the argument ssid leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	2026-06-08	8.8	CVE-2026-11503
Tenda--CX12L	A vulnerability was detected in Tenda CX12L 16.03.53.12. The impacted element is the function setSchedWifi of the file /goform/openSchedWifi of the component Wi-Fi Schedule Configuration Endpoint. Performing a manipulation of the argument schedStartTime/schedEndTime results in stack-based buffer overflow. The attack may be initiated remotely. The exploit is now public and may be used.	2026-06-08	8.8	CVE-2026-11504
Tenda--F451	A security flaw has been discovered in Tenda F451 1.0.0.7/1.0.0.9. Impacted is the function formWriteFacMac of the file /goform/WriteFacMac of the component Web Management Interface. Performing a manipulation of the argument mac results in os command injection. Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.	2026-06-08	8.8	CVE-2026-11556
Tenda--F451	A weakness has been identified in Tenda F451 1.0.0.7/1.0.0.9. The affected element is the function fromNatlimit of the file /goform/Natlimit of the component Web Management Interface. Executing a manipulation of the argument page can lead to stack-based buffer overflow. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	2026-06-08	8.8	CVE-2026-11557
Tenda--HG7HG9	A vulnerability was determined in Tenda HG7HG9 and HG10 300001138_en_xpon. This affects the function formDOMAINBLK of the file /boaform/formDOMAINBLK. Executing a manipulation of the argument blkDomain can lead to stack-based buffer overflow. The attack may be performed from remote.	2026-06-08	9.8	CVE-2026-11499
Tenda--HG7HG9	A vulnerability was found in Tenda HG7HG9 and HG10 300001138_en_xpon. Affected by this issue is the function asp_voip_OtherSet of the file /boaform/voip_other_set of the component Web Management Interface. Performing a manipulation of the argument funckey_transfer results in stack-based buffer overflow. The attack is possible to be carried out remotely.	2026-06-08	8.8	CVE-2026-11498
Tenda--HG7HG9	A vulnerability was found in Tenda HG7HG9 and HG10 300001138_en_xpon. This affects the function formPPPEdit of the file /boaform/formPPPEdit. The manipulation of the argument encodename results in stack-based buffer overflow. The attack can be launched remotely. The exploit has been made public and could be used.	2026-06-08	8.8	CVE-2026-11553
Tenda--W20E	A vulnerability was detected in Tenda W20E 15.11.0.6. This vulnerability affects the function formSetPortMirror of the file /goform/setPortMirror. Performing a manipulation of the argument portMirrorMirroredPorts	2026-06-08	8.8	CVE-2026-11522

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	results in stack-based buffer overflow. The attack can be initiated remotely. The exploit is now public and may be used.			
Tenda--W20E	A flaw has been found in Tenda W20E 15.11.0.6. This issue affects the function formPortalAuth of the file /goform/PortalAuth of the component Web Management Interface. Executing a manipulation of the argument gotoUrl can lead to stack-based buffer overflow. The attack can be launched remotely. The exploit has been published and may be used.	2026-06-08	8.8	CVE-2026-11523
Tenda--W20E	A vulnerability has been found in Tenda W20E 15.11.0.6. Impacted is the function modifyWifiFilterRules of the file /goform/modifyWifiFilterRules of the component Web Management Interface. The manipulation of the argument wifiFilterListRemark leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2026-06-08	8.8	CVE-2026-11524
Themeisle--Woody Code Snippets	WordPress Insert PHP plugin versions before 3.3.1 contain a PHP code injection vulnerability that allows unauthenticated attackers to execute arbitrary PHP code by injecting malicious shortcodes through the WordPress REST API. Attackers can send POST requests to the wp-json/wp/v2/posts endpoint with crafted content containing insert_php shortcodes to include and execute remote PHP files on the server.	2026-06-09	9.8	CVE-2017-20251
Ubiquiti Inc--UDM	Under certain network configurations, a malicious actor with access to network could exploit an Improper Access Control vulnerability found in certain devices running UniFi OS to make unauthorized changes to such UniFi OS devices.	2026-06-12	8.1	CVE-2026-48610
Ubiquiti Inc--UID Enterprise Agent	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UID Enterprise Agent to execute a Command Injection on the host device.	2026-06-12	9.9	CVE-2026-47367
Ubiquiti Inc--UniFi OS Server	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in certain devices running UniFi OS to escalate privileges within such UniFi OS devices or instances.	2026-06-12	9.9	CVE-2026-47369
Ubiquiti Inc--UniFi OS Server	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in certain devices running UniFi OS to execute a Command Injection within such UniFi OS devices or instances.	2026-06-12	9.9	CVE-2026-47370
Ubiquiti Inc--UniFi OS Server	A malicious actor with access to the network could exploit a Path Traversal vulnerability found in certain devices running UniFi OS to obtain data from such UniFi OS devices or instances.	2026-06-12	8.6	CVE-2026-47368
UTT--HiPER 2610G	A vulnerability was determined in UTT HiPER 2610G up to 3.0.0-171107. This impacts the function strcopy of the file /goform/formConfigDnsFilterGlobal. Executing a manipulation of the argument GroupName can lead to buffer overflow. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	2026-06-08	8.8	CVE-2026-11517
VMware--VCF operations	VMware Cloud Foundation Operations contains multiple stored cross-site scripting vulnerabilities.A malicious actor with privileges to create policies, views or text-widgets may be able to inject scripts to perform administrative actions in VMware Cloud Foundation Operations.	2026-06-08	8	CVE-2026-41722
VMware--VCF operations	VMware Cloud Foundation Operations contains multiple stored cross-site scripting vulnerabilities.A malicious actor with privileges to create policies, views or text-widgets may be able to inject scripts to perform administrative actions in VMware Cloud Foundation Operations.	2026-06-08	8	CVE-2026-41723
VMware--VCF operations	VMware Cloud Foundation Operations contains multiple stored cross-site scripting vulnerabilities.A malicious actor with privileges to create policies, views or text-widgets may be able to inject scripts to perform administrative actions in VMware Cloud Foundation Operations.	2026-06-08	8	CVE-2026-41724
VS Revo--RevoUninstaller	A vulnerability was identified in VS Revo RevoUninstaller 2.5.x/2.6.x. The affected element is the function IOCTL_Handler in the library RevoDetector.sys of the component IOCTL Handler. Such manipulation	2026-06-14	7.8	CVE-2026-12193

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	leads to heap-based buffer overflow. The attack must be carried out locally. The exploit is publicly available and might be used. Upgrading to version 2.7.0 is sufficient to fix this issue. It is recommended to upgrade the affected component.			
WBW Plugins-- Product Filter by WBW	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WBW Plugins Product Filter by WBW allows Blind SQL Injection. This issue affects Product Filter by WBW: from n/a through 3.1.2.	2026-06-11	9.3	CVE-2026-39494
webandprint-- Augmented Reality	WordPress Augmented-Reality plugin contains a remote code execution vulnerability in the elFinder connector that allows unauthenticated attackers to upload and execute arbitrary PHP files. Attackers can send POST requests to the connector.minimal.php endpoint with mkfile and put commands to create malicious PHP files in the file_manager directory and execute them on the server.	2026-06-08	7.5	CVE-2023-54350
WebPros-- WordPress-Toolkit	Argument injection vulnerability in WordPress Toolkit before 6.11.0 as used in cPanel & WHM, allows remote authenticated users to bypass cross-tenant authorization and execute arbitrary wp-toolkit CLI commands as another account.	2026-06-12	9.9	CVE-2026-47365
Wow-Company-- Wow Forms	Wow Forms WordPress Plugin version 2.1 contains an SQL injection vulnerability that allows unauthenticated attackers to read arbitrary database information by exploiting an unescaped POST parameter. Attackers can inject SQL code through the 'mwpformid' parameter in requests to the admin-ajax.php endpoint with the 'send_mwp_form' action to extract sensitive database contents.	2026-06-09	8.2	CVE-2017-20244
Wow-Company-- Wow Viral Signups	Wow Viral Signups 2.1 WordPress plugin contains an SQL injection vulnerability that allows unauthenticated attackers to extract database information by exploiting the unescaped 'idsignup' POST parameter. Attackers can send crafted requests to the admin-ajax.php endpoint with malicious SQL payloads in the 'idsignup' parameter to read arbitrary data from the database.	2026-06-09	8.2	CVE-2017-20245
WP Travel Kit-- Travelscape	WordPress Seotheme contains a remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary PHP code by uploading malicious files to the theme directory. Attackers can access the uploaded PHP shell at /wp-content/themes/seotheme/mar.php to execute system commands and upload additional files for persistent access.	2026-06-08	9.8	CVE-2023-54352
WP Travel Kit-- Travelscape	WordPress Theme Travelscape 1.0.3 contains an arbitrary file upload vulnerability that allows unauthenticated attackers to upload malicious files by exploiting insufficient validation in the theme's upload functionality. Attackers can upload arbitrary files to the theme directory and execute them to achieve remote code execution on the affected WordPress installation.	2026-06-08	9.8	CVE-2024-58349
WPVibes--WP Mail Log	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in WPVibes WP Mail Log allows DOM-Based XSS. This issue affects WP Mail Log: from n/a through 1.0.2.	2026-06-11	7.1	CVE-2023-33999
WPZOOM-- WPZOOM Portfolio	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPZOOM Portfolio allows Reflected XSS. This issue affects WPZOOM Portfolio: from n/a through 1.4.21.	2026-06-10	7.1	CVE-2026-49069
xibosignage-- xibo-cms	Xibo is an open source digital signage platform with a web content management system and Windows display player software. Prior to 4.4.2, a vulnerability chain consisting of Stored XSS and Iframe Sandbox escape in the Xibo CMS allows users with DataSet permissions to use the Data Connector functionality to craft messages which escape the sandbox and facilitate XSS. Exploitation of the vulnerability is possible on behalf of an authorized user who has both of the following privileges, which are not granted to non-admins as standard: Include "Add DataSet" button to allow for additional DataSets to be created independently to Layouts Users should upgrade to version 4.4.2 which fixes this issue. Upgrading to a fixed version is necessary to remediate. Users unable to upgrade should revoke such privileges from users they do not trust.	2026-06-10	7.6	CVE-2026-42558

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Yarbo--Yarbo Android/iOS mobile application	The Yarbo Android and iOS applications contain hard-coded MQTT broker credentials that are identical for all users and all devices. These credentials are embedded in the application binary and are readily extractable via APK decompilation. The credentials provide access to cloud MQTT brokers carrying real-time telemetry for the entire global Yarbo robot fleet. They allow both wildcard subscription to all robot telemetry topics and publishing to any robot's command topic using only the robot's serial number.	2026-06-12	9.8	CVE-2026-10557
Yarbo--Yarbo Android/iOS mobile application	The Yarbo cloud does not enforce per-device or per-user authorization. Any client possessing valid credentials, whether the shared hard-coded credentials or legitimate per-user credentials, can subscribe to wildcard topics covering all robots globally, and can publish to any robot's command topic using only the robot's serial number (disclosed in the telemetry stream). Even after removal of hard-coded credentials from the app, a single compromised credential could still provide fleet-wide access without per-device access controls.	2026-06-12	8.1	CVE-2026-7368
YesWiki--yeswiki	YesWiki is a wiki system written in PHP. Prior to version 4.6.6, an unsafe execution vulnerability exists in the Bazar form field calculator (CalcField.php) of YesWiki. The application attempts to sanitize user-defined mathematical formulas using a complex recursive regular expression before passing them to the PHP eval() function. This implementation is inherently flawed: it is vulnerable to Regular Expression Denial of Service (ReDoS / Stack Overflow) which can crash the server, and it creates a high-risk architecture where any logic bypass directly results in arbitrary PHP code execution. Version 4.6.6 patches the issue.	2026-06-08	9.8	CVE-2026-52778
zephyrproject-rtos--Zephyr	A remote, unauthenticated attacker can trigger memory corruption in Zephyr's HTTP server WebSocket upgrade path by sending a crafted Sec-WebSocket-Key header. The HTTP/1 header parser copies the header into a fixed-size buffer using a bounded copy that does not guarantee NUL termination when the input length reaches the buffer size. During upgrade handling the buffer is copied to a local stack buffer and passed to strlen(); if no NUL exists in-bounds, strlen() reads beyond the stack buffer and subsequent concatenation with the WebSocket magic string can write out of bounds. This leads to out-of-bounds read and write on stack memory, resulting in crash (denial of service) and potentially code execution. The path is reachable when CONFIG_HTTP_SERVER_WEBSOCKET is enabled.	2026-06-09	9.8	CVE-2026-5067
zephyrproject-rtos--Zephyr	A remote, unauthenticated BLE peer can trigger a 2-byte out-of-bounds write in the Bluetooth host during L2CAP LE CoC SDU reassembly. When the application enables segmentation (via chan_ops.alloc_buf) and the chosen RX pool has a user_data_size smaller than 2 bytes, the segmentation counter stored in the net_buf user_data area is written out of bounds in l2cap_chan_le_recv_seg (subsys/bluetooth/host/l2cap.c). The observed effects are an AddressSanitizer abort and, without ASan, heap corruption / fatal error.	2026-06-09	7.6	CVE-2026-5068
Zoom Communications --Remote Control for Zoom Contact Center	Insufficient Verification of Data Authenticity in Remote Control for Zoom Contact Center for Windows before version 7.0.0 may allow an authenticated user to enable an escalation of privilege via local access.	2026-06-12	7.8	CVE-2026-53406
Zoom Communications --Zoom Workplace	Improper Authorization in Handler for Custom URL Scheme in Zoom Workplace before version 7.0.4 for Android and before 7.0.3 for iOS may allow an unauthenticated user to conduct an escalation of privilege via network access.	2026-06-12	8.1	CVE-2026-53407
Zoom Communications --Zoom Workplace	Improper Authorization in Handler for Custom URL Scheme in Zoom Workplace before version 7.0.4 for Android and before 7.0.3 for iOS may allow an unauthenticated user to conduct an escalation of privilege via network access.	2026-06-12	8.1	CVE-2026-53408
10Web--Form Maker by 10Web	Unauthenticated SQL Injection in Form Maker by 10Web <= 1.15.38 versions.	2026-06-15	9.3	CVE-2026-39502

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
404-redirection-manager--404 Redirection Manager	The 404 Redirection Manager plugin version 1.0 for WordPress contains an unauthenticated SQL injection vulnerability that allows remote attackers to execute arbitrary SQL queries by injecting malicious code through unsanitized user input. Attackers can craft GET requests with SQL injection payloads to manipulate database queries and extract sensitive information from the WordPress database.	2026-06-15	8.2	CVE-2016-20071
A WP Life--Webenvo	Subscriber Arbitrary File Upload in Webenvo <= 0.0.6 versions.	2026-06-17	9.9	CVE-2026-39589
AA-Team--Premium Age Verification / Restriction for WordPress	Unauthenticated Arbitrary File Download in Premium Age Verification / Restriction for WordPress <= 3.0.2 versions.	2026-06-17	7.5	CVE-2025-49403
ACPT--ACPT (Pro) - Custom Post Types Plugin for WordPress	Improper Control of Generation of Code ('Code Injection') vulnerability in ACPT ACPT (Pro) - Custom Post Types Plugin for WordPress allows Remote Code Inclusion. This issue affects ACPT (Pro) - Custom Post Types Plugin for WordPress: from n/a through 2.0.47.	2026-06-16	10	CVE-2026-25470
activity-log.com--WP Sessions Time Monitoring Full Automatic	Subscriber SQL Injection in WP Sessions Time Monitoring Full Automatic <= 1.1.4 versions.	2026-06-16	8.5	CVE-2026-39581
Adobe--Adobe Acrobat PDF Extension (Chrome)	Adobe Acrobat PDF Extension (Chrome) versions 26.5.2.2 and earlier are affected by a UXSS-class cross-origin data disclosure vulnerability. An attacker could exploit this vulnerability to gain access to data regarding the victim's session. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.	2026-06-16	7.4	CVE-2026-48294
Adobe--DNG SDK	DNG SDK versions 1.7.1 2536 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-16	7.8	CVE-2026-47964
Advanced Ads GmbH--Advanced Ads Tracking	Unauthenticated SQL Injection in Advanced Ads - Tracking < 3.0.7 versions.	2026-06-17	9.3	CVE-2025-59554
aguilatechnologies--WP Customer Area	Custom role Path Traversal in WP Customer Area <= 8.3.4 versions.	2026-06-15	8.8	CVE-2026-42661
Ahmad--GeekyBot	Unauthenticated Arbitrary File Upload in GeekyBot <= 1.2.2 versions.	2026-06-15	10	CVE-2026-40772
Ahmad--GeekyBot	Unauthenticated SQL Injection in GeekyBot <= 1.2.0 versions.	2026-06-15	9.3	CVE-2026-39519
Ahmad--JS Help Desk	Unauthenticated SQL Injection in JS Help Desk <= 3.0.9 versions.	2026-06-15	9.3	CVE-2026-48886
AivahThemes--Car Zone	Unauthenticated Arbitrary File Deletion in Car Zone <= 3.7 versions.	2026-06-16	8.6	CVE-2025-69139
AI Monsor--ABC Crypto Checkout	Unauthenticated Sensitive Data Exposure in ABC Crypto Checkout <= 1.8.2 versions.	2026-06-15	7.5	CVE-2026-52695
Alberto Hornero--Clean Login	Unauthenticated Insecure Direct Object References (IDOR) in Clean Login <= 1.15 versions.	2026-06-17	8.2	CVE-2026-54184
Aman--FunnelKit Automations	Subscriber Broken Authentication in FunnelKit Automations <= 3.7.3 versions.	2026-06-15	7.1	CVE-2026-39450
Anydesk--AnyDesk	AnyDesk 2.5.0 contains an unquoted service path vulnerability that allows local users to execute arbitrary code with SYSTEM privileges by exploiting the service installation. Attackers can insert malicious executables in the system root path that execute with elevated privileges during application startup or system reboot.	2026-06-19	7.8	CVE-2016-20094

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
AOMEI--Backupper	A vulnerability was determined in AOMEI Backupper up to 8.3.0. Impacted is an unknown function in the library amwrtdrv.sys of the component Kernel Driver. Executing a manipulation can lead to improper access controls. The attack needs to be launched locally. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	7.8	CVE-2026-12780
AOMEI--Dynamic Disk Manager	A vulnerability was found in AOMEI Dynamic Disk Manager up to 10.10.1. This issue affects some unknown processing in the library ddmdrv.sys of the component Kernel Driver. Performing a manipulation results in improper access controls. The attack must be initiated from a local position. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	7.8	CVE-2026-12779
AOMEI--Partition Assistant	A vulnerability has been found in AOMEI Partition Assistant up to 10.10.1. This vulnerability affects unknown code in the library ampa10.sys of the component Kernel Driver. Such manipulation leads to improper access controls. The attack must be carried out locally. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	7.8	CVE-2026-12778
Archetyped--Favicon Rotator	Unauthenticated Cross Site Scripting (XSS) in Favicon Rotator <= 1.2.11 versions.	2026-06-15	7.1	CVE-2026-42649
ArrayHQ--Okay Toolkit	Unauthenticated Cross Site Scripting (XSS) in Okay Toolkit <= 2.3 versions.	2026-06-15	7.1	CVE-2025-68851
Arraytics--WP Event SOLution	Unauthenticated Broken Access Control in WP Event SOLution <= 4.1.12 versions.	2026-06-16	7.5	CVE-2025-68045
Arraytics--WP Event SOLution	Unauthenticated Broken Access Control in WP Event SOLution <= 4.1.8 versions.	2026-06-15	7.5	CVE-2026-40776
artbees--JupiterX Core	Unauthenticated Broken Access Control in JupiterX Core <= 4.14.1 versions.	2026-06-16	7.5	CVE-2026-39490
Artio--Joomla! com_booking component	Joomla com_booking component 2.4.9 contains an information disclosure vulnerability that allows unauthenticated attackers to enumerate user accounts by exploiting the getUserData function in the customer controller. Attackers can send GET requests to index.php with option=com_booking, controller=customer, task=getUserData, and an id parameter to retrieve user names, usernames, and email addresses through brute force enumeration.	2026-06-19	7.5	CVE-2023-54357
Avast--AVAST Antivirus	AVAST Antivirus 25.11 contains an unquoted service path vulnerability in the SecureLine service that allows local non-privileged users to execute code with elevated SYSTEM privileges. Attackers can exploit the unquoted binary path in the service configuration to inject malicious executables that execute with high-level system permissions.	2026-06-19	7.8	CVE-2025-71326
AVer--PTC500S	Improper input validation in AVer PTC500S, PTC115, PTC500+, and PTC115+ cameras may allow a remote, unauthenticated attacker to achieve arbitrary code execution via a specially crafted web request.	2026-06-18	9.8	CVE-2026-40624
AVideo--AVideo	AVideo through 29.0 contains an authorization bypass vulnerability in the Meet plugin's uploadRecordedVideo.json.php endpoint that derives the target users_id from the uploaded filename without verification. An attacker with knowledge of the Meet shared secret can craft a malicious file upload with a filename containing an arbitrary users_id to invoke passwordless User->login() and establish an authenticated session as any user including admin. Attackers can obtain the Meet shared secret through path-traversal vulnerabilities or timing attacks against checkToken.json.php, then POST a crafted file to uploadRecordedVideo.json.php with a filename like '1-anything.mp4' to hijack admin sessions and gain full account takeover.	2026-06-20	8.1	CVE-2026-56345
AVideo--AVideo	AVideo through version 26.0 contains multiple unauthenticated list.json.php endpoints in payment plugins lacking authorization checks, exposing PayPal tokens, Authorize.Net webhooks, and Bitcoin transaction records. Unauthenticated attackers can retrieve all payment transaction	2026-06-20	7.5	CVE-2026-56341

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	data including agreement IDs, user financial records, and API responses via direct GET requests to vulnerable endpoints.			
Awesomemotive--Contact Form by WPForms	Unauthenticated Broken Access Control in Contact Form by WPForms <= 1.10.0.4 versions.	2026-06-15	7.5	CVE-2026-48835
Awesomemotive--Easy Digital Downloads	Unauthenticated Broken Access Control in Easy Digital Downloads <= 3.6.5 versions.	2026-06-15	7.5	CVE-2026-39503
AWS--bedrock-agentcore	Improper neutralization of argument delimiters in the install_packages() method in AWS Bedrock AgentCore Python SDK versions >= 1.1.3 and < 1.6.1 might allow a remote authenticated user to execute arbitrary commands within the Code Interpreter sandbox via crafted package name arguments. To mitigate this issue, users should upgrade to version 1.6.1.	2026-06-17	7.3	CVE-2026-12530
AxiomThemes--Promo	Unauthenticated Local File Inclusion in Promo <= 1.3.0 versions.	2026-06-17	8.1	CVE-2026-22325
AxiomThemes--Reprizo	Unauthenticated Local File Inclusion in Reprizo <= 1.0.8 versions.	2026-06-17	8.1	CVE-2026-22326
Ays Pro--Popup box	Unauthenticated Cross Site Scripting (XSS) in Popup box <= 6.2.9 versions.	2026-06-17	7.1	CVE-2026-54192
Azuriom--Azuriom CMS	Missing Authorization in the server management routes (routes/admin.php) in Azuriom Azuriom CMS before 1.2.11 on all platforms allows an authenticated attacker with the admin.access permission to create AzLink server tokens and take over non-admin user accounts by changing their passwords and email addresses via crafted HTTP requests to /admin/servers/create and the AzLink API endpoints (/api/azlink/password, /api/azlink/email, /api/azlink/user/{id}).	2026-06-17	8.1	CVE-2026-54415
baptisteArno--typebot.io	TypeBot is a chatbot builder tool. In versions 3.16.1 and earlier, POST /api/blocks/file-input/v3/generate-upload-url is unauthenticated and uses unsanitized fileName input to construct public/ S3 object keys, while issuing presigned PUT URLs that do not bind Content-Type. As a result, any anonymous visitor to a published bot with a file input can upload attacker-controlled HTML, SVG, or JS to attacker-chosen subpaths, including other tenants' publicly served result paths, enabling arbitrary content hosting and potential stored XSS on the storage origin. ../ traversal is blocked by S3/MinIO canonicalization (signature mismatch), but forward-slash path injection is exploitable. This issue has been fixed in version 3.17.0.	2026-06-17	9.3	CVE-2026-48768
baptisteArno--typebot.io	TypeBot is a chatbot builder tool. In versions prior to 3.17.2, SSRF validation is implemented by resolving a hostname once and checking whether the resolved IP belongs to a forbidden range allowing for DNS rebinding bypass. The root cause is a time-of-check to time-of-use gap in the SSRF guard. The validator resolves the hostname and approves it, but the later request path performs a fresh resolution and connects to whatever IP the hostname maps to at that moment. The actual outbound request is then performed later using the original hostname, without pinning the validated IP to the network connection. An attacker who can supply a URL to a public bot that performs a server-side HTTP Request block or server-side script fetch can use DNS rebinding to pass the initial validation and still force the server to connect to a private or metadata address during the real request. This enables server-side access to private network services, cloud metadata endpoints, and other internal HTTP targets that the validator was intended to block. The exact downstream impact depends on the reachable internal services. Concrete consequences include metadata disclosure, access to internal admin panels, credential theft from metadata services, and further compromise through internal-only HTTP interfaces. This issue has been fixed in version 3.17.2.	2026-06-17	8.2	CVE-2026-48764
baptisteArno--typebot.io	TypeBot is a chatbot builder tool. Versions 3.15.2 and below have an Insecure Direct Object Reference vulnerability through cross-workspace Theme Template modification and deletion. The	2026-06-17	7.1	CVE-2026-48759

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	handleSaveThemeTemplate and handleDeleteThemeTemplate handlers validate that the authenticated user is a non-guest member of the provided workspaceId, but then operate on themeTemplateId via Prisma queries that do NOT include workspaceId in the WHERE clause. This allows any authenticated user to modify or delete theme templates belonging to any other workspace and may expose Template IDs via shared typebots or network traffic. This issue has been fixed in version 3.16.0.			
Barn2 Media Ltd--WooCommerce Product Filters	Unauthenticated PHP Object Injection in WooCommerce Product Filters < 2.0.6 versions.	2026-06-17	9.8	CVE-2026-40725
bbsetheme--BBS e-Franchise	BBS e-Franchise 1.1.1 plugin for WordPress contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the uid parameter. Attackers can craft requests to pages using the plugin's shortcode with UNION-based SQL injection in the uid parameter to extract sensitive data from the WordPress database including user information and taxonomy terms.	2026-06-15	8.2	CVE-2016-20072
BdThemes--Element Pack Pro	Contributor Local File Inclusion in Element Pack Pro <= 9.0.6 versions.	2026-06-17	7.5	CVE-2026-40721
BDthemes--SigmaForms Pro AI Generated Forms	Unauthenticated Arbitrary File Upload in SigmaForms Pro - AI Generated Forms <= 1.4.5 versions.	2026-06-17	9	CVE-2026-52705
BerriAI--litellm	A weakness has been identified in BerriAI litellm up to 1.59.8. Affected is the function UserAPIKeyAuth of the file litellm/proxy/_experimental/mcp_server/auth/user_api_key_auth_mcp.py of the component MCP Proxy. Executing a manipulation can lead to improper authentication. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure.	2026-06-21	7.3	CVE-2026-12773
BerriAI--litellm	A vulnerability was determined in BerriAI litellm up to 1.82.2. This affects the function json.dumps of the file litellm/proxy/management_endpoints/ui_sso.py of the component SSO Debug Flow. Executing a manipulation can lead to missing authentication. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure.	2026-06-21	7.3	CVE-2026-12795
betterdocs--BetterDocs Pro	The BetterDocs Pro plugin for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 3.8.0 via the `doc_style` parameter. This makes it possible for unauthenticated attackers to include and execute arbitrary .php files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where .php file types can be uploaded and included.	2026-06-19	9.8	CVE-2026-7515
bgermann--CformsII	Unauthenticated Cross Site Scripting (XSS) in CformsII <= 15.1.3 versions.	2026-06-15	7.1	CVE-2026-39435
Bhavin Thummar--Product Filter Widget for Elementor	Unauthenticated Cross Site Scripting (XSS) in Product Filter Widget for Elementor <= 1.0.6 versions.	2026-06-15	7.1	CVE-2026-45437
Binisoft--Windows Firewall Control	Windows Firewall Control 4.8.6.0 contains an unquoted service path vulnerability that allows local attackers to escalate privileges by inserting malicious executables in the service path. Attackers can place executable files in unquoted path directories that the wfcs.exe service will execute with LocalSystem privileges upon service restart or system reboot.	2026-06-19	7.8	CVE-2016-20091

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Bitnami--bitnami/cassandra	Bitnami Cassandra container images are affected by a retained default superuser vulnerability. When a custom administrator account is configured via the CASSANDRA_USER environment variable, the container initialization script creates the new superuser account but fails to drop the built-in cassandra account in certain scenarios. This leaves the default cassandra:cassandra superuser active as an unintended access path. Affected versions - Container image: 4.0.x prior to 4.0.20-photon-5-r7; 4.1.x prior to 4.1.11-photon-5-r7; 5.0.x prior to 5.0.8-photon-5-r4 / 5.0.8-debian-12-r3.	2026-06-18	9.8	CVE-2026-47846
Blubrry Podcasting--PowerPress Podcasting	Contributor SQL Injection in PowerPress Podcasting <= 11.15.10 versions.	2026-06-15	8.5	CVE-2026-24637
BoldThemes--Nifty	Unauthenticated PHP Object Injection in Nifty <= 1.4.1 versions.	2026-06-16	9.8	CVE-2026-27429
Bookly--Bookly	Unauthenticated Sensitive Data Exposure in Bookly <= 27.4 versions.	2026-06-15	7.5	CVE-2026-42667
bPlugins--B Blocks	Contributor Privilege Escalation in B Blocks <= 2.0.31 versions.	2026-06-15	8.8	CVE-2026-39579
Brainstorm Force--OttoKit	Unauthenticated PHP Object Injection in OttoKit <= 1.1.27 versions.	2026-06-15	9.8	CVE-2026-49781
Brainstorm Force--SureDash	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Brainstorm Force SureDash allows Blind SQL Injection. This issue affects SureDash: from n/a through 1.8.0.	2026-06-17	8.5	CVE-2026-54813
Brainstorm Force--WooCommerce Cart Abandonment Recovery	Shop manager Privilege Escalation in WooCommerce Cart Abandonment Recovery < 2.1.0 versions.	2026-06-15	7.2	CVE-2026-39470
Bricksforge--Bricksforge	Unauthenticated Sensitive Data Exposure in Bricksforge <= 3.1.8.4 versions.	2026-06-17	7.5	CVE-2026-34888
Brother--SAPSprint	Brother SAPSprint 7.60 contains an unquoted service path vulnerability in the SAPSprint service binary that allows local attackers to escalate privileges. Attackers can place a malicious executable in the Program Files directory path to be executed with LocalSystem privileges when the service starts automatically.	2026-06-19	7.8	CVE-2021-47985
browserstack--browserstack-cypress-cli	The browserstack-cypress-cli is BrowserStack's CLI which allows users to run Cypress tests on BrowserStack. Versions prior to 1.36.4 are vulnerable to OS command injection via the cypress_config_file configuration parameter. In readCypressConfigUtil.js, the loadJsFile() function constructs a shell command by interpolating the user-controlled cypress_config_filepath value into a template literal, then executes it via child_process.execSync(). Shell metacharacters in the config path (specifically " and ;) allow breaking out of the quoted argument and injecting arbitrary commands. This issue has been fixed in version 1.36.6.	2026-06-15	7.8	CVE-2026-48723
bytecodealliance--wasmtime	Wasmtime is a runtime for WebAssembly. In versions prior to 24.0.9, 36.0.10, and 44.0.2, when a filesystem preopen is given DirPerms::all() and FilePerms::READ without FilePerms::WRITE, this access control mechanism can be bypassed via the wasip2 descriptor.open-at or wasip1 path_open interfaces by opening a file with only the OpenFlags::TRUNCATE oflag. The root cause is that the clause handling OpenFlags::TRUNCATE in crates/wasi/src/filesystem.rs (Dir::open_at, lines 967-969) did not set open_mode = OpenMode::WRITE;, which is later used for the access control check against FilePerms to determine whether opening the file is permitted; the single-line fix adds that missing assignment, after which the affected calls correctly fail with error-code.not-permitted and ERRNO_PERM respectively. Only wasmtime-wasi embeddings that combine DirPerms::MUTATE with FilePerms::READ are affected by this	2026-06-15	7.5	CVE-2026-47261

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bug. In particular, the Wasmtime project's wasmtime-cli's use of wasmtime-wasi is not affected, because it always sets FilePerms::all() for all preopens. This issue has been fixed in versions 24.0.9, 36.0.10 and 44.0.2.			
CactusThemes--Truemag	Unauthenticated Local File Inclusion in Truemag <= 4.3.14.2 versions.	2026-06-16	8.1	CVE-2025-69178
Cap-go--capgo	Cap-go before 12.128.2 contains an authentication bypass vulnerability in OTP verification that allows attackers to bypass email verification by modifying server responses. Attackers can intercept OTP verification requests and manipulate HTTP responses to falsely mark verification successful, enabling unauthorized 2FA enablement and account takeover.	2026-06-19	9.4	CVE-2026-56073
Cap-go--capgo	Cap-go before 12.128.2 contains an authentication logic flaw that lets an attacker register and control an account bound to a victim's email address before that email is verified. By enabling two-factor authentication on the pre-registered account, the attacker gains control over the account claimed under the victim's identity, allowing them to read and modify its state and enforce organization-level policies, while the legitimate user is denied access to the account tied to their own email.	2026-06-19	9.1	CVE-2026-56081
Cap-go--capgo	Capgo (Cap-go/capgo) before 12.128.2 contains an improper access control vulnerability in the SECURITY DEFINER PostgREST RPC function public.record_build_time, which is granted to the anon role and callable with only the public Supabase publishable (sb_publishable_*) anon key. An unauthenticated attacker can insert rows into public.build_logs for arbitrary organizations and, because the function uses ON CONFLICT (build_id, org_id) DO UPDATE, can overwrite existing usage/billing records by reusing the same build_id for a target org. This enables cross-tenant tampering of billing build logs and financial-impact denial of service by inflating billable build time.	2026-06-19	7.5	CVE-2026-56082
Capgo--Capgo	Capgo before 12.128.12 allows authenticated users to modify their mutable public.users.email to arbitrary addresses, which the SSO provisioning endpoint trusts as an account-merge key. Attackers can pre-position their account with a victim's corporate SSO email, causing the provision-user endpoint to merge the victim's SSO identity into the attacker-controlled account.	2026-06-20	8.3	CVE-2026-56215
Capgo--Capgo	Capgo before 12.128.2 contains a scope escalation vulnerability in the POST /functions/v1/apikey endpoint that allows app-limited API keys to mint unrestricted keys by setting empty limits. Attackers with a compromised app-limited key can create an unrestricted key with org-wide access to resources like app listings and other protected endpoints.	2026-06-20	8.8	CVE-2026-56216
Capgo--Capgo	Capgo before 12.128.2 contains an information disclosure vulnerability in Supabase PostgREST RPC endpoints is_trial_org and is_paying_org that allows unauthenticated attackers to enumerate organizations and disclose billing status using the public sb_publishable key. Attackers can invoke these endpoints to determine organization existence via distinguishable return values and identify paying customers for targeted profiling.	2026-06-20	7.5	CVE-2026-56214
Capgo--Capgo	Capgo before 12.128.2 contains a potential privilege escalation vulnerability in the public.apply_usage_overage SECURITY DEFINER function, which performs sensitive billing operations without enforcing internal authorization checks (no validation of auth.uid(), org membership, or check_min_rights). Because the function runs with the owner's privileges, it bypasses Row Level Security. If EXECUTE permission is available to the authenticated or anon roles (explicitly or via default privileges), an authenticated user could invoke it via Supabase RPC to manipulate billing data for arbitrary organizations, including unauthorized credit depletion and fraudulent overage event insertion.	2026-06-21	7.6	CVE-2026-56239
Capgo--Capgo	Capgo before 12.128.2 contains an unauthenticated security definer RPC function get_identity_apikey_only that returns the owning user_id for supplied API keys, creating an API key validity oracle and user identity disclosure primitive. Attackers can call this endpoint with valid or invalid	2026-06-21	7.5	CVE-2026-56242

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	API keys to confirm key validity and map keys to user identifiers, then chain results into other exposed RPCs like get_orgs_v6 to retrieve organization membership and management email PII.			
Capgo--Capgo	Capgo before 12.128.2 contains an improper access control vulnerability in the public.get_org_members RPC function that allows unauthenticated attackers to enumerate organization members. Attackers can invoke the endpoint using only the public sb_publishable_* key and an organization UUID to retrieve sensitive member information including email addresses, user IDs, roles, and pending invitations.	2026-06-21	7.5	CVE-2026-56253
Cargo RD--Cargo Shipping Location for WooCommerce	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Cargo RD Cargo Shipping Location for WooCommerce allows Blind SQL Injection. This issue affects Cargo Shipping Location for WooCommerce: from n/a through 5.6.	2026-06-17	9.3	CVE-2026-54815
Chatway Live Chat--Chatway Live Chat " AI Chatbot, Customer Support, FAQ & Helpdesk Customer Service & Chat Buttons	Subscriber Sensitive Data Exposure in Chatway Live Chat – AI Chatbot, Customer Support, FAQ & Helpdesk Customer Service & Chat Buttons <= 1.4.8 versions.	2026-06-15	7.4	CVE-2026-49082
Cherryframework--Cherry Framework Themes	WordPress CherryFramework Themes 3.1.4 contains an information disclosure vulnerability that allows unauthenticated attackers to download sensitive backup files by accessing the download_backup.php endpoint. Attackers can directly access the download_backup.php script in the admin/data_management directory to obtain ZIP archives containing the entire wp-content/themes directory contents.	2026-06-15	7.5	CVE-2018-25437
ChrisHurst--Simple Backup	WordPress Simple-Backup 2.7.11 contains multiple vulnerabilities that allow unauthenticated attackers to delete arbitrary files and download sensitive files by manipulating the delete_backup_file and download_backup_file parameters in tools.php. Attackers can exploit insufficient input validation using directory traversal techniques to access wp-config.php, database dumps, and other sensitive files, or delete critical files .htaccess to expose backup directories.	2026-06-15	7.5	CVE-2016-20076
Cisco--Cisco Identity Services Engine Software	A vulnerability in Cisco ISE and ISE-PIC could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have valid administrative credentials. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root. In single-node deployments, successful exploitation of this vulnerability could cause the affected ISE node to become unavailable, resulting in a denial of service (DoS) condition. In that condition, endpoints that have not already authenticated would be unable to access the network until the node is restored.	2026-06-17	9.1	CVE-2026-20181
Cisco--Cisco Identity Services Engine Software	A vulnerability in Cisco ISE and ISE-PIC could allow an unauthenticated, remote attacker to view sensitive information on an affected device. This vulnerability is due to improper authorization checks when a resource is accessed. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to sensitive information, including hashed credentials that could be used in future attacks.	2026-06-17	7.5	CVE-2026-20190
claudiopizzillo--PIAF-HMS	claudiopizzillo PIAF-HMS (PBX-In-A-Flash Hotel Management System; no released versions, latest commit 389d2633441b65ced1c104212cd62be2bfca21e5) contains multiple	2026-06-18	9.8	CVE-2026-54419

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthenticated SQL injection vulnerabilities. The application has no authentication mechanism and passes user-supplied HTTP parameters directly into deprecated mysql_query() calls via string concatenation, without sanitization, escaping, or parameterization. Affected sinks include rooms.php (DELETE FROM Rooms WHERE ID = \$_GET['ID'], unquoted numeric context), checkuser.php (WHERE Ext = '\$_GET["Ext"]'), ec.php (date/extension parameters in a WHERE), checkin.php and wakeup.php (\$_POST values into INSERT statements), bills.php (\$_POST fields built into a WHERE clause), and rates.php and checkout.php. A remote, unauthenticated attacker can inject arbitrary SQL to read, modify, or delete arbitrary records in the backing database (e.g. rooms.php?ID=1 OR 1=1 deletes all room records). Note: queries run via the legacy mysql_* extension, which does not permit stacked statements.			
CMSJunkie WordPress Business Directory Plugins--WP-BusinessDirectory	Subscriber Arbitrary File Upload in WP-BusinessDirectory <= 4.0.0 versions.	2026-06-15	9.9	CVE-2026-39591
Cmsjunkie--ClassifiedsManager	Joomla Component J-ClassifiedsManager 3.0.5 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through POST parameters. Attackers can submit crafted SQL payloads in the categorySearch, adType, and citySearch parameters to the displayads component to extract sensitive database information including usernames, databases, and version details.	2026-06-19	8.2	CVE-2019-25751
Cmsjunkie--J-BusinessDirectory	Joomla! Component J-BusinessDirectory 4.9.7 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the type parameter. Attackers can send GET requests to index.php with the option=com_jbusinessdirectory&task=categories.getCategories parameters and inject UNION-based SQL statements in the type parameter to extract database information including schema names and sensitive data.	2026-06-19	8.2	CVE-2019-25752
Cmsjunkie--J-CruisePortal	Joomla J-CruisePortal 6.0.4 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the guest_adult parameter. Attackers can send POST requests to the cruises endpoint with crafted SQL payloads in the guest_adult parameter to extract sensitive database information or manipulate database records.	2026-06-19	7.1	CVE-2019-25749
Cmsjunkie--JHotelReservation	Joomla JHotelReservation 6.0.7 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the rooms parameter. Attackers can send POST requests to the search-hotels endpoint with crafted SQL payloads in the rooms parameter to extract sensitive database information including version details.	2026-06-19	8.2	CVE-2019-25748
Cmsjunkie--MultipleHotelReservation	Joomla Component J-MultipleHotelReservation 6.0.7 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the hotel_id parameter. Attackers can send POST requests to the search-hotels endpoint with crafted SQL UNION SELECT statements to extract sensitive database information including table names and column data.	2026-06-19	8.2	CVE-2019-25750
codepeople--WP Time Slots Booking Form	Subscriber SQL Injection in WP Time Slots Booking Form <= 1.2.50 versions.	2026-06-15	8.5	CVE-2026-48882
codepeople--WP Time Slots Booking Form	Unauthenticated Cross Site Scripting (XSS) in WP Time Slots Booking Form <= 1.2.46 versions.	2026-06-15	7.1	CVE-2026-40791

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codesupplyco--Uppercase	Unauthenticated Local File Inclusion in Uppercase < 1.2.2 versions.	2026-06-17	8.1	CVE-2026-39559
collectchat--collectchat	Unauthenticated Cross Site Scripting (XSS) in collectchat <= 2.4.9 versions.	2026-06-17	7.1	CVE-2026-40765
cometd--cometd	CometD is a scalable comet implementation for web messaging. In versions 5.0.0 through 5.0.22, 6.0.0 through 6.0.18, 7.0.0 through 7.0.18, and 8.0.0 through 8.0.8, bad clients that always send a fixed batch value when the server is using the acknowledgement extension may cause the unacknowledged message queue to grow indefinitely, eventually causing an 'OutOfMemoryError'. Versions 5.0.23, 6.0.19, 7.0.19, and 8.0.9 patch the issue. As a workaround, disable the acknowledgement extension.	2026-06-18	7.5	CVE-2025-53114
Comodo--Chromodo Browser	Comodo Chromodo Browser 52.15.25.664 contains an unquoted service path vulnerability in the ChromodoUpdater service that runs with SYSTEM privileges. A local attacker can insert a malicious executable in the service path and execute arbitrary code with elevated privileges upon service restart or system reboot.	2026-06-19	7.8	CVE-2016-20088
Comodo--Dragon Browser	Comodo Dragon Browser versions up to 52.15.25.663 contain a privilege escalation vulnerability in the DragonUpdater service due to an unquoted service path running with SYSTEM privileges. A local attacker can insert a malicious executable in the service path and execute arbitrary code with elevated privileges upon service restart or system reboot.	2026-06-19	7.8	CVE-2016-20090
conda-forge--conda-smithy	conda-smithy is a tool for combining a conda recipe with configurations to build using freely hosted CI services into a single repository. Prior to version 3.61.0, a vulnerability in the conda-forge automated webservices allowed unintended write access to feedstock repositories through GitHub username takeover. The root cause is the use of mutable GitHub usernames as identifiers for repository invitation routing, rather than stable, immutable GitHub user IDs. Version 3.61.0 fixes the issue.	2026-06-18	7.6	CVE-2026-46699
Conekta Group--Conekta Payment Gateway	Unauthenticated Sensitive Data Exposure in Conekta Payment Gateway <= 6.0.0 versions.	2026-06-15	7.5	CVE-2026-49066
contest-gallery--Contest Gallery Upload & Vote Photos, Media, Sell with PayPal & Stripe	The Contest Gallery - Upload & Vote Photos, Media, Sell with PayPal & Stripe plugin for WordPress is vulnerable to Privilege Escalation in all versions up to, and including, 30.0.2 via the 'RegistryUserRole' parameter. This is due to the plugin's admin menu being registered at the 'edit_posts' capability level - granting Contributor-level users access to the plugin's admin pages and a valid 'cg_admin' nonce - while the option-saving handler in 'change-options-and-sizes.php' performs no 'current_user_can()' capability check beyond 'check_admin_referer('cg_admin')', and the 'RegistryUserRole' value is processed only through 'sanitize_text_field()' and 'htmlentities()' without restriction to an allowlist of permitted role names. This makes it possible for authenticated attackers, with author-level access and above, to overwrite the plugin's stored 'RegistryUserRole' option with 'administrator', which the 'cg_create_wp_user_from_google_user' function then reads back from the 'contest_gallery_registry_and_login_options' database table without any allowlist validation and passes directly to 'wp_update_user()', effectively promoting a newly registered Google sign-in account to Administrator.	2026-06-17	8.8	CVE-2026-12165
Cotonti--Cotonti	Cotonti 1.0.0 (master branch, commit f43f1fc3) is vulnerable to Cross-Site Request Forgery in the administration rights handler. In system/admin/admin.rights.php, the rights update action ('a=update') modifies group access rights (including via cot_auth_add_group) without calling cot_check_xg() to validate the anti-CSRF token. A remote attacker who lures an authenticated administrator into visiting a malicious page can force the browser to submit a forged request that grants elevated permissions to an attacker-controlled group, escalating privileges to administrator. Because Cotonti administrators can modify templates and	2026-06-18	9.6	CVE-2026-55742

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	configuration, this can be further leveraged toward remote code execution.			
Cotonti--Cotonti	Cotonti 1.0.0 (master branch, commit f43f1fc3) is vulnerable to Cross-Site Request Forgery in the administration configuration handler. In system/admin/admin.config.php, the configuration update action ('a=update') processes POST data via cot_config_update_options() without calling cot_check_xg() to validate the anti-CSRF token (the 'x' parameter), unlike other admin handlers (e.g. admin.structure.php, admin.cache.php). A remote attacker who lures an authenticated administrator into visiting a malicious page can force the browser to submit a forged request that modifies arbitrary core, module, or plugin configuration options, which can be leveraged to weaken security or enable further compromise.	2026-06-18	8.8	CVE-2026-55741
Cotonti--Cotonti	Cotonti 1.0.0 (master branch, commit f43f1fc3) is vulnerable to Cross-Site Request Forgery in the Personal File Storage (PFS) module. In modules/pfs/inc/pfs.main.php, the file upload action ('a=upload') processes uploaded files without calling cot_check_xg() to validate the anti-CSRF token, even though sibling actions such as 'delete' (line 272) do. A remote attacker who lures an authenticated user into visiting a malicious page can force the browser to submit a forged multipart request that uploads arbitrary files into the victim's PFS storage.	2026-06-18	8.1	CVE-2026-55744
Cotonti--Cotonti	Cotonti 1.0.0 (master branch, commit f43f1fc3) is vulnerable to stored Cross-Site Scripting in the Personal File Storage (PFS) module. A folder title (pff_title) is imported with the 'TXT' filter, which does not strip or encode HTML (the tag check in cot_import is disabled), so an authenticated user can store HTML/JavaScript in a folder title. In modules/pfs/inc/pfs.main.php the title is assigned to the template variable PFF_ROW_TITLE without htmlspecialchars(), and modules/pfs/tpl/pfs.tpl outputs {PFF_ROW_TITLE} unescaped. When the folder listing is viewed (including by other users for public folders), the injected script executes in the victim's browser.	2026-06-18	7.6	CVE-2026-55746
coturn--coturn	Coturn is a free open source implementation of TURN and STUN Server. Versions prior to 4.10.0 contain a stack buffer overflow in decode_oauth_token_gcm(). A uint16_t nonce_len field read from an attacker-supplied OAuth access token (0-65535) is passed directly to memcpy() as the copy length into a 256-byte stack buffer (oauth_encrypted_block.nonce[256]) without bounds checking. The overflow occurs before AES-GCM authentication is verified, the attacker does not need to know the OAuth key or produce a valid AES-GCM token. Up to 735 bytes of attacker-controlled data are written past the buffer, may corrupt adjacent stack data, including control-flow data depending on compiler, ABI, and mitigations. Requires --oauth mode (non-default). This may provide a plausible RCE primitive depending on exploit mitigations; because coturn is widely deployed for WebRTC TURN/STUN and --oauth is commonly recommended, impact can be broad. This issue has been fixed in version 4.10.0.	2026-06-18	8.1	CVE-2026-43994
Cozmoslabs--Paid Member Subscriptions	Unauthenticated Cross Site Scripting (XSS) in Paid Member Subscriptions <= 2.17.3 versions.	2026-06-15	7.1	CVE-2026-39514
Cozmoslabs--Profile Builder Pro	Unauthenticated Cross Site Scripting (XSS) in Profile Builder Pro <= 3.15.0 versions.	2026-06-17	7.1	CVE-2026-42385
Cozy Vision Technologies Pvt. Ltd.--SMS Alert Order Notifications	Subscriber Privilege Escalation in SMS Alert Order Notifications <= 3.9.4 versions.	2026-06-17	9.8	CVE-2026-54803
Cozy Vision Technologies Pvt. Ltd.--SMS	Unauthenticated Broken Authentication in SMS Alert Order Notifications <= 3.9.3 versions.	2026-06-17	7.5	CVE-2026-54802

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Alert Order Notifications				
craftcms--cms	Craft CMS (composer package craftcms/cms) versions >= 5.5.0 and <= 5.9.13 contain a remote code execution vulnerability in the FieldsController::actionRenderCardPreview() method, which passes the fieldLayoutConfig POST parameter directly to Fields::createLayout() without calling Component::cleanseConfig(). An authenticated admin user can inject Yii2 event handlers (e.g., 'on init' keys) via the fieldLayoutConfig parameter to execute arbitrary PHP code and disclose sensitive information (such as environment variables containing database credentials and CRAFT_SECURITY_KEY). The issue is fixed in version 5.9.14.	2026-06-21	7.2	CVE-2026-56382
Crawl4AI--Crawl4AI	Crawl4AI before 0.8.7 contains an authentication bypass vulnerability due to a hardcoded default JWT signing key in the Docker API server. Attackers who know the default key can forge valid authentication tokens for any user, bypassing authentication and gaining full access to protected functionality.	2026-06-21	9.8	CVE-2026-56265
Creative Themes--Blocksy Companion Pro	Unauthenticated SQL Injection in Blocksy Companion Pro < 2.1.29 versions.	2026-06-17	9.3	CVE-2026-39596
Creative Themes--Blocksy Companion Pro	Contributor Remote Code Execution (RCE) in Blocksy Companion Pro <= 2.1.37 versions.	2026-06-17	9.9	CVE-2026-40783
CRM Perks--Integration for ActiveCampaign and Contact Form 7, WPForms, Elementor, Ninja Forms	Unauthenticated PHP Object Injection in Integration for ActiveCampaign and Contact Form 7, WPForms, Elementor, Ninja Forms <= 1.1.1 versions.	2026-06-15	9.8	CVE-2026-9691
CRM Perks--Integration for Contact Form 7 and Constant Contact	Unauthenticated PHP Object Injection in Integration for Contact Form 7 and Constant Contact <= 1.1.6 versions.	2026-06-15	9.8	CVE-2026-49106
CRM Perks--Integration for Contact Form 7 HubSpot	Unauthenticated PHP Object Injection in Integration for Contact Form 7 HubSpot <= 1.3.7 versions.	2026-06-15	9.8	CVE-2026-49763
CRM Perks--Integration for Keap/infusionsoft and Contact Form 7, WPForms, Elementor, Formidable, Ninja Forms	Unauthenticated PHP Object Injection in Integration for Keap/infusionsoft and Contact Form 7, WPForms, Elementor, Formidable, Ninja Forms <= 1.2.1 versions.	2026-06-15	9.8	CVE-2026-49104
CRM Perks--Integration for Mailchimp and Contact Form 7, WPForms, Elementor, Ninja Forms	Unauthenticated PHP Object Injection in Integration for Mailchimp and Contact Form 7, WPForms, Elementor, Ninja Forms <= 1.1.8 versions.	2026-06-15	9.8	CVE-2026-49765
crm perks--Integration for Salesforce and Contact Form 7,	Unauthenticated PHP Object Injection in Integration for Salesforce and Contact Form 7, WPForms, Elementor, Formidable, Ninja Forms <= 1.4.3 versions.	2026-06-15	9.8	CVE-2026-49109

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WPForms, Elementor, Formidable, Ninja Forms				
CRM Perks--WP Insightly for Contact Form 7, WPForms, Elementor, Formidable and Ninja Forms	Unauthenticated PHP Object Injection in WP Insightly for Contact Form 7, WPForms, Elementor, Formidable and Ninja Forms <= 1.1.4 versions.	2026-06-15	9.8	CVE-2026-49085
CRM Perks--WP Zendesk for Contact Form 7, WPForms, Elementor, Formidable and Ninja Forms	Unauthenticated PHP Object Injection in WP Zendesk for Contact Form 7, WPForms, Elementor, Formidable and Ninja Forms <= 1.1.4 versions.	2026-06-15	9.8	CVE-2026-49105
crmpers--Database for Contact Form 7, WPforms, Elementor forms	The Database for Contact Form 7, WPforms, Elementor forms plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the view_page function in all versions up to, and including, 1.5.1. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). Successful exploitation requires an administrator to view or edit the poisoned form entry, at which point PHP's bracket parser reshapes the attacker-crafted JSON key to bypass the stored-path isset check and trigger deletion of the traversal-specified file.	2026-06-20	8.1	CVE-2026-9843
Crocoblock--JetEngine	The JetEngine plugin for WordPress is vulnerable to SQL injection in all versions up to and including 3.8.10.1. The listing_load_more AJAX handler accepts a filtered_query parameter that is intentionally excluded from the HMAC query signature check to support front-end filter integration. However, meta_query row values within filtered_query are not sanitized before being merged into SQL construction. This makes it possible for unauthenticated attackers to perform time-based or boolean blind SQL injection by appending a malicious meta_query value to a Load More AJAX request captured from any public Listing Grid page.	2026-06-17	7.5	CVE-2026-12360
CurlyThemes--Events Schedule - WordPress Events Calendar Plugin	Subscriber SQL Injection in Events Schedule - WordPress Events Calendar Plugin <= 2.7.2 versions.	2026-06-17	8.5	CVE-2025-69135
Dassault Systmes--SOLIDWORKS Visualize	A Path Traversal vulnerability affecting SOLIDWORKS Visualize from SOLIDWORKS Desktop Release 2024 through SOLIDWORKS Desktop Release 2026 could allow an attacker to write arbitrary files on the server.	2026-06-17	9.8	CVE-2026-10094
Datalogics--Datalogics Ecommerce Delivery	Unauthenticated Privilege Escalation in Datalogics Ecommerce Delivery <= 2.6.62 versions.	2026-06-15	9.8	CVE-2026-39583
David Lingren--Media Library Assistant	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in David Lingren Media Library Assistant allows Blind SQL Injection. This issue affects Media Library Assistant: from n/a through 3.35.	2026-06-18	8.5	CVE-2026-56012
David Lingren--Media Library Assistant	Unauthenticated Cross Site Scripting (XSS) in Media Library Assistant <= 3.35 versions.	2026-06-16	7.1	CVE-2026-54198
dbgate--dbgate	DbGate is cross-platform database manager. In versions 7.1.8 and prior, the POST /runners/load-reader endpoint in DbGate accepts a	2026-06-15	8.8	CVE-2026-48017

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	functionName parameter that is directly interpolated into a JavaScript code template without any sanitization or validation. An authenticated user (with basic access, no special permissions required) can inject arbitrary JavaScript code that executes on the server with full process privileges, bypassing the require=null sandbox restriction. An authenticated user with basic access (no admin role, no run-shell-script permission required) can: execute arbitrary OS commands on the DbGate server with the privileges of the Node.js process, read/write any file accessible to the process, pivot to connected databases by reading connection credentials from DbGate's storage, and compromise the host system - in Docker deployments, this typically means root access within the container.			
deepstreamIO--deepstream.io	deepstream is a server that allows clients and backend services to sync data, send messages and make rpcs at scale. Versions prior to 10.0.5 are vulnerable to Prototype Pollution. Exploitation can lead to potential privilege escalation from any authenticated user with write permission to any record. This issue has been fixed in version 10.0.5.	2026-06-18	9.9	CVE-2026-49252
Dell--AIOps	Dell AIOps Collector versions prior to 1.18.3 contain a "Use of Default Credentials" vulnerability. A low privileged attacker with console access could potentially exploit this vulnerability to gain Filesystem access. This vulnerability only affects fresh installations of Collector versions earlier than 1.18.3. Systems that have been upgraded (either manually or automatically) to version 1.18.3 or later are not impacted, even if they were originally installed on an earlier version.	2026-06-17	7.8	CVE-2026-32652
Dell--Dell EMC VxRail Appliance	update_disk_psu_baseline.sh requires password in plain text	2026-06-16	7.4	CVE-2024-39575
Dell--EMC VxRail Appliance	api-gateway container running with root privilege would allow an attacker to escape the container and access host system to perform unintended actions.	2026-06-16	7	CVE-2024-38487
Dell--OpenManage	Dell OpenManage Integration with Microsoft Windows Admin Center contains a Remote Code Execution vulnerability in the gateway plugin. A remote authenticated user could potentially exploit this vulnerability to escalate privileges. The malicious user may gain the ability to run arbitrary code remotely. This is a high severity vulnerability so Dell recommends customers to upgrade at the earliest opportunity.	2026-06-16	8.8	CVE-2024-24909
Dell--PowerFlex	Dell PowerFlex Manager, version(s) [Versions], contain(s) an Improper Authentication vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Unauthorized access.	2026-06-17	8.1	CVE-2026-32804
Dell--PowerFlex	Dell PowerFlex Manager, version(s) [Versions], contain(s) a Missing Authentication for Critical Function vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Code execution, Denial of service, Information disclosure, Information tampering, Remote execution, Script injection, and Unauthorized access.	2026-06-17	8.8	CVE-2026-35065
Dell--PowerFlex	Dell PowerFlex Manager, version(s) Version prior to 4.8, contain(s) an Inclusion of Functionality from Untrusted Control Sphere vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	2026-06-17	7.5	CVE-2026-22283
Dell--PowerFlex	Dell PowerFlex Manager, version(s) [Versions], contain(s) an Improper Access Control vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to denial of service.	2026-06-17	7.1	CVE-2026-35066
Dell--PowerFlex	Dell PowerFlex Manager, version(s) [Versions], contain(s) an Improper Authentication vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Information disclosure, Information tampering, and Unauthorized access.	2026-06-17	7.4	CVE-2026-49502
Dell--Server Hardware Manager	Dell Server Hardware Manager, versions prior to 3.2.2, contains an Improper Access Control vulnerability. A low privileged attacker with local	2026-06-19	7.8	CVE-2026-46461

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	access could potentially exploit this vulnerability, leading to Elevation of privileges.			
Dev4Press--GD Rating System	Unauthenticated SQL Injection in GD Rating System <= 3.6.2 versions.	2026-06-15	9.3	CVE-2026-42639
Dimitri Grassi--Salon booking system	Unauthenticated Insecure Direct Object References (IDOR) in Salon booking system <= 10.30.24 versions.	2026-06-17	7.3	CVE-2026-40768
Dimitri Grassi--Salon booking system	Unauthenticated Broken Access Control in Salon booking system <= 10.30.25 versions.	2026-06-15	7.5	CVE-2026-42666
Discuz!--Discuz! X5.0	Discuz! X5.0 releases 20260320 through 20260501 contains an authentication bypass vulnerability that allows unauthenticated remote attackers to gain unauthorized access to database backup and restore functionality by exploiting a shared cryptographic key between UCenter integration and the database backup API exposed by dbbak.php. Attackers can inject a crafted payload through the username parameter during login to abuse the encryption oracle in logging_ctl::logging_more(), obtain a legitimately signed token, and use it to bypass authorization for database export and import operations, with the additional ability to trigger a race condition to impersonate arbitrary users.	2026-06-15	9.1	CVE-2026-49952
Discuz!--Discuz! X5.0	Discuz! X5.0 releases 20260320 through 20260610 contain a local file inclusion vulnerability that allows authenticated administrators to execute arbitrary code by importing a specially crafted plugin configuration containing path traversal sequences in the directory attribute. Attackers can trigger an exception during plugin installation to bypass sanitization routines, causing malicious paths to be stored unsanitized and subsequently passed to include(), which combined with file upload functionality escalates to arbitrary code execution in the context of the web server user.	2026-06-15	7.2	CVE-2026-49954
Dokan, Inc.--Dokan	Customer Privilege Escalation in Dokan <= 5.0.2 versions.	2026-06-15	8.8	CVE-2026-49780
doobidoo--mcp-memory-service	mcp-memory-service is a semantic memory layer for AI applications. Prior to version 10.65.3, the HTTP MCP JSON-RPC endpoint at `/mcp` requires only OAuth `read` scope for all requests, then dispatches `tools/call` directly to handlers that include mutating tools. A read-only OAuth client can call `store_memory` and `delete_memory` through MCP even though the corresponding REST endpoints require `write` scope. Version 10.65.3 patches the issue.	2026-06-19	8.1	CVE-2026-49291
DVDFab--Virtual Drive	A security vulnerability has been detected in DVDFab Virtual Drive 2.0.0.5. Impacted is an unknown function in the library dvdfabio.sys of the component Signed Kernel Driver. The manipulation leads to improper privilege management. An attack has to be approached locally. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	7.8	CVE-2026-12217
dwbooster--Booking Calendar Contact	WordPress appointment-booking-calendar 1.1.24 contains multiple privilege escalation vulnerabilities that allow unauthenticated attackers to modify calendar settings and inject persistent cross-site scripting payloads through the admin.php page parameters. Attackers can inject malicious JavaScript into the 'ict' and 'ics' options or the calendar 'name' parameter via GET requests to execute arbitrary scripts when the calendar is displayed or accessed in the administration interface.	2026-06-15	7.2	CVE-2016-20084
dwbooster--Booking Calendar Contact Form	WordPress Booking Calendar Contact Form version 1.0.23 contains an unauthenticated blind SQL injection vulnerability that allows remote attackers to execute arbitrary SQL queries by injecting malicious code through the 'id' parameter. Attackers can send requests to the admin-ajax.php endpoint with the action parameter set to 'dex_bccf_calendar_ajaxevent' and supply crafted SQL commands in the 'id' parameter to extract sensitive database information.	2026-06-15	8.2	CVE-2016-20068

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dwbooster--Booking Calendar Contact Form	WordPress Booking Calendar Contact Form 1.0.23 contains an unauthenticated blind SQL injection vulnerability in the shortcode function that fails to sanitize the calendar parameter before using it in database queries. Attackers can inject SQL commands through the calendar shortcode parameter to execute arbitrary SQL queries and extract sensitive database information.	2026-06-15	8.2	CVE-2016-20069
dwbooster--CP Polls	WordPress CP Polls 1.0.8 contains a persistent cross-site scripting vulnerability that allows attackers to inject malicious scripts through unsanitized file upload functionality. Attackers can upload files containing script payloads with event handlers like onerror attributes to execute arbitrary JavaScript in the browsers of users viewing the affected content.	2026-06-15	7.2	CVE-2016-20066
Dylan Kuhn--Geo Mashup	Subscriber SQL Injection in Geo Mashup <= 1.13.19 versions.	2026-06-17	8.5	CVE-2026-48967
e107inc--e107	e107 is a content management system (CMS). Versions 2.3.5 and earlier contain a command injection vulnerability in the ImageMagick resize destination path. In resize_image(), the source path is escaped with escapeshellarg(), but the destination path is inserted inside raw double quotes in the convert command; in the submit-news upload flow, that destination filename includes the first six characters of user-controlled news title input. Because the title filter removes literal spaces but not tab characters, and shell expansions such as \$(...) and backticks can survive into the quoted destination argument, /bin/sh -c may evaluate attacker-controlled input. Exploitation is possible only when all of the following non-default settings are enabled: resize_method=ImageMagick, subnews_attach=1, upload_enabled=1, subnews_resize is numeric between 30 and 5000, and the attacker is a non-admin in classes permitted by both subnews_class and upload_class. This issue has been fixed in version 2.3.6.	2026-06-17	7.1	CVE-2026-48997
e4jvikwp--VikRentCar	Unauthenticated Insecure Direct Object References (IDOR) in VikRentCar <= 1.4.5 versions.	2026-06-15	7.5	CVE-2026-52699
EaseUS--Partition Master	A vulnerability was identified in EaseUS Partition Master up to 14.5. The affected element is an unknown function in the library epmntdrv.sys of the component Kernel Driver. The manipulation leads to improper access controls. The attack needs to be performed locally. The exploit is publicly available and might be used. You should upgrade the affected component. The vendor explains: "We have confirmed that this issue was present only in older versions of the product. Our product has since been updated, and the issue has been resolved in the latest version, so it no longer exists."	2026-06-21	7.8	CVE-2026-12781
EaseUS--Partition Master	A security flaw has been discovered in EaseUS Partition Master up to 14.5. The impacted element is an unknown function in the library EUEDKEPM.sys of the component Kernel Driver. The manipulation results in improper access controls. The attack requires a local approach. The exploit has been released to the public and may be used for attacks. The affected component should be upgraded. The vendor explains: "We have confirmed that this issue was present only in older versions of the product. Our product has since been updated, and the issue has been resolved in the latest version, so it no longer exists."	2026-06-21	7.8	CVE-2026-12782
Easy Appointments--Easy Appointments	Unauthenticated Broken Access Control in Easy Appointments <= 3.12.21 versions.	2026-06-15	7.5	CVE-2026-39513
Eclipse Foundation--Eclipse ThreadX - NetX Duo	The security fix for CVE-2025-0728 in eclipse-threadx NetX Duo refactors error handling in the HTTP server PUT process to use a shared cleanup label, but this unified cleanup path unconditionally calls fx_file_close() even when the file was never successfully opened. Multiple error branches jump to the shared cleanup label before any file open operation has occurred, causing fx_file_close() to operate on an uninitialized file handle, leading to undefined behavior, double-close issues, or memory corruption.	2026-06-19	7.5	CVE-2026-11576

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Edgar Rojas--WooCommerce PDF Invoice Builder	Improper Control of Generation of Code ('Code Injection') vulnerability in Edgar Rojas WooCommerce PDF Invoice Builder allows Remote Code Inclusion. This issue affects WooCommerce PDF Invoice Builder: from n/a through 2.0.8.	2026-06-15	10	CVE-2026-52704
Edge-Themes--Alloggio - Hotel Booking	Unauthenticated PHP Object Injection in Alloggio - Hotel Booking <= 2.1.2 versions.	2026-06-16	8.1	CVE-2026-39539
Edge-Themes--Behold	Unauthenticated PHP Object Injection in Behold <= 1.5 versions.	2026-06-16	8.1	CVE-2026-40760
Edge-Themes--Eldon	Unauthenticated PHP Object Injection in Eldon <= 1.4.1 versions.	2026-06-17	8.1	CVE-2026-40738
Edge-Themes--Laurits	Unauthenticated PHP Object Injection in Laurits <= 1.5.1 versions.	2026-06-16	8.1	CVE-2026-40736
Edge-Themes--Reina	Unauthenticated PHP Object Injection in Reina <= 2.1 versions.	2026-06-17	8.1	CVE-2026-40735
Edge-Themes--Valeska	Unauthenticated PHP Object Injection in Valeska <= 1.2.2 versions.	2026-06-16	8.1	CVE-2026-40761
Edimax--BR-6478AC V2	A vulnerability has been found in Edimax BR-6478AC V2 1.23. The impacted element is the function formWISiteSurvey of the file /goform/formWISiteSurvey of the component POST Request Handler. The manipulation of the argument selSSID leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	8.8	CVE-2026-12806
eemitch--Simple File List	The Simple File List plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the eeSFL_DeleteFile function in all versions up to, and including, 6.3.7. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). The simplefilelist_edit_job AJAX action is registered via wp_ajax_nopriv_, making it accessible without authentication, and the is_admin() guard that would otherwise restrict access is bypassed because is_admin() always returns true for requests to the admin-ajax.php endpoint.	2026-06-20	7.5	CVE-2026-11911
eemitch--Simple File List	The Simple File List plugin for WordPress is vulnerable to arbitrary file modification due to insufficient authorization checks in all versions up to, and including, 6.3.7. This makes it possible for unauthenticated attackers to delete and modify files on the server. This vulnerability is exploitable even when the administrator has not enabled the AllowFrontManage setting, because the is_admin() check unconditionally short-circuits the guard before that setting is evaluated.	2026-06-20	7.5	CVE-2026-11912
Elated-Themes--Aperitif	Unauthenticated Local File Inclusion in Aperitif <= 1.5 versions.	2026-06-16	8.1	CVE-2026-39549
Elated-Themes--Fidalgo	Unauthenticated PHP Object Injection in Fidalgo <= 1.2.2 versions.	2026-06-16	8.1	CVE-2026-39554
Elated-Themes--Konsept	Unauthenticated PHP Object Injection in Konsept <= 1.9 versions.	2026-06-17	8.1	CVE-2026-39556
Elated-Themes--Lonie	Unauthenticated PHP Object Injection in LÃ©onie <= 1.2.1 versions.	2026-06-16	8.1	CVE-2026-40758
Elated-Themes--Malm	Unauthenticated Local File Inclusion in Malm <= 2.2 versions.	2026-06-17	8.1	CVE-2026-39558
Elated-Themes--Mr. SEO	Unauthenticated Local File Inclusion in Mr. SEO <= 2.0 versions.	2026-06-16	8.1	CVE-2026-39568
Elated-Themes--NeoBeat	Unauthenticated PHP Object Injection in NeoBeat <= 1.7 versions.	2026-06-16	8.1	CVE-2026-39557
Elated-Themes--Playroom	Unauthenticated PHP Object Injection in Playroom <= 1.4.1 versions.	2026-06-16	8.1	CVE-2026-39577

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Elated-Themes--Roisin	Unauthenticated PHP Object Injection in Roisin <= 1.4 versions.	2026-06-16	8.1	CVE-2026-40754
Elated-Themes--SingleMalt	Unauthenticated PHP Object Injection in SingleMalt <= 1.5 versions.	2026-06-17	8.1	CVE-2026-39576
Elated-Themes--Solene	Unauthenticated Local File Inclusion in Solene <= 3.4 versions.	2026-06-16	8.1	CVE-2026-39522
Elated-Themes--Solene Core	Unauthenticated Local File Inclusion in Solene Core <= 2.3.2 versions.	2026-06-17	8.1	CVE-2026-39523
Elated-Themes--Valiance	Unauthenticated PHP Object Injection in Valiance <= 1.2 versions.	2026-06-16	8.1	CVE-2026-39578
ELEXtensions--ELEX WordPress HelpDesk & Customer Ticketing System	Subscriber SQL Injection in ELEX WordPress HelpDesk & Customer Ticketing System <= 3.3.6 versions.	2026-06-15	8.5	CVE-2026-48964
Eli Scheetz--Anti-Malware Security and Brute-Force Firewall	Contributor PHP Object Injection in Anti-Malware Security and Brute-Force Firewall <= 4.23.87 versions.	2026-06-15	8.8	CVE-2026-39478
Eli--Eli's WordCents adSense Widget with Analytics	Unauthenticated Cross Site Scripting (XSS) in Eli's WordCents adSense Widget with Analytics <= 1.3.03.27 versions.	2026-06-15	7.1	CVE-2025-68872
Emraan Cheema--ListingPro	Unauthenticated SQL Injection in ListingPro <= 2.9.10 versions.	2026-06-16	9.3	CVE-2026-39438
EMV--Creatify	Deserialization of Untrusted Data vulnerability in EMV Creatify allows Object Injection. This issue affects Creatify: from n/a through 1.5.	2026-06-17	9.8	CVE-2025-60236
EMV--JobBank	Missing Authorization vulnerability in EMV JobBank allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects JobBank: from n/a through 1.2.3.	2026-06-17	7.3	CVE-2025-69189
EMV--JobCareer	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in EMV JobCareer allows Path Traversal. This issue affects JobCareer: from n/a through 7.3.	2026-06-17	8.6	CVE-2025-69128
EMV--The Hospital	Deserialization of Untrusted Data vulnerability in EMV The Hospital nrghospital allows Object Injection. This issue affects The Hospital: from n/a through 1.8.1.	2026-06-17	9.8	CVE-2025-60231
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to versions 1.35.11, 1.36.7, 1.37.3, and 1.38.1, a vulnerability in Envoy's HTTP/2 downstream request processing allows an unauthenticated remote client to trigger excessive memory consumption, potentially resulting in OOM termination of the Envoy process and denial of service. The issue arises from the combination of two behaviors. First, cookie header bytes are not fully accounted for during request header size validation in Envoy. Second, HPACK header block limits in oghttp2/quiche are enforced on encoded bytes without a corresponding limit on total decoded header size. Together, these behaviors allow a malicious client to cause large decoded header allocations while bypassing the intended request header size protections. Versions 1.35.11, 1.36.7, 1.37.3, and 1.38.1 contain a fix. No complete workaround is known short of applying a fix. Possible temporary mitigations include disabling downstream HTTP/2 where operationally feasible; enforcing stricter request header and cookie limits before traffic reaches Envoy; and monitoring Envoy memory usage for abnormal growth under HTTP/2 traffic.	2026-06-17	7.5	CVE-2026-47774
error311--FileRise	FileRise before 3.16.0 is vulnerable to path traversal in the shared-folder upload endpoint (/api/folder/uploadToSharedFolder.php), leading to arbitrary file write and administrator account takeover. The upload filename is validated by FolderController with basename() and	2026-06-19	9.8	CVE-2026-54414

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	REGEX_FILE_NAME, which permit URL-encoded sequences (the regex blocks / and \ but not %). The raw filename is then passed to UploadModel::handleUpload, where it is reconstructed as trim(urldecode(basename(\$fileName))), re-introducing path separators after validation (e.g. ../%2fusers%2fusers.txt becomes ../users/users.txt). UploadNamePolicy::isAllowedForWrite() applies basename() internally and therefore only evaluates the final component (users.txt), allowing the traversal sequence to pass the extension policy. The destination path is then used directly in move_uploaded_file() with no realpath containment check, allowing a write outside the intended upload directory. An attacker who possesses a valid, non-expired, upload-enabled shared-folder link/token (which are designed to be shared publicly) can overwrite users/users.txt to create an administrator account, resulting in unauthenticated admin takeover and, depending on configuration, remote code execution. Exploitation requires possession of a valid, non-expired, upload-enabled shared-folder link/token. This issue is fixed in 3.16.0, which URL-decodes before validation and rejects any path separators in the upload filename.			
Etoilewebdesign--Ultimate Product Catalog	WordPress Ultimate Product Catalog 3.8.6 contains an arbitrary file upload vulnerability that allows authenticated users with contributor, editor, author, or administrator roles to upload malicious files by exploiting the custom fields functionality. Attackers can upload PHP shells through the Products tab custom file field and access them via the upcp-product-file-uploads directory to execute arbitrary code on the server.	2026-06-15	8.8	CVE-2016-20075
EventPrime--EventPrime	Unauthenticated PHP Object Injection in EventPrime <= 4.3.2.1 versions.	2026-06-15	8.1	CVE-2026-42687
EventPrime--EventPrime	Subscriber Insecure Direct Object References (IDOR) in EventPrime <= 4.3.0.0 versions.	2026-06-15	7.1	CVE-2026-39518
EventPrime--EventPrime	Subscriber Cross Site Scripting (XSS) in EventPrime <= 4.3.2.1 versions.	2026-06-15	7.1	CVE-2026-42686
ExpressTech--Quiz And Survey Master	Unauthenticated Cross Site Scripting (XSS) in Quiz And Survey Master <= 11.0.0 versions.	2026-06-15	7.1	CVE-2026-40787
ExpressTech--Quiz And Survey Master	Unauthenticated Cross Site Scripting (XSS) in Quiz And Survey Master <= 11.1.2 versions.	2026-06-15	7.1	CVE-2026-48867
Extendons--WordPress & WooCommerce Scraper Plugin, Import Data from Any Site	Unauthenticated Arbitrary File Upload in WordPress & WooCommerce Scraper Plugin, Import Data from Any Site <= 1.0.7 versions.	2026-06-17	10	CVE-2025-69129
extendons--WordPress & WooCommerce Scraper Plugin, Import Data from Any Site	Unauthenticated Arbitrary File Download in WordPress & WooCommerce Scraper Plugin, Import Data from Any Site <= 1.0.7 versions.	2026-06-16	7.5	CVE-2025-69131
Extensions--Joomla Payage	Joomla Payage 2.05 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the aid parameter. Attackers can send GET requests to index.php with malicious aid values in the make_payment task to extract sensitive database information using boolean-based blind or time-based blind techniques.	2026-06-19	8.2	CVE-2017-20279
Extro--RPC	Joomla! Component RPC Responsive Portfolio 1.6.1 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send GET requests to index.php with	2026-06-19	8.2	CVE-2017-20258

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	option=com_pofos&view=pofo&id=[SQL] to extract sensitive database information.			
Eyal Fitoussi-- GEO my WordPress	Unauthenticated SQL Injection in GEO my WordPress <= 4.5.5 versions.	2026-06-16	9.3	CVE-2026-52715
EyeCix Technologies-- JobSearch	Unauthenticated Broken Access Control in JobSearch <= 3.2.7 versions.	2026-06-16	7.5	CVE-2026-49057
eyecix-- JobSearch	Unauthenticated SQL Injection in JobSearch <= 3.2.9 versions.	2026-06-17	9.3	CVE-2026-54186
Ezbsystems-- UltraISO Premium Edition	A vulnerability has been found in Ezbsystems UltraISO Premium Edition up to 9.76. Affected by this issue is some unknown functionality in the library bootpt64.sys of the component Kernel Driver. The manipulation leads to improper access controls. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	7.8	CVE-2026-12786
F5--NGINX Gateway Fabric	When NGINX Plus is configured as the data plane for NGINX Gateway Fabric, an injection vulnerability exists in the NGINX configuration generator component of NGINX Gateway Fabric. User-supplied string values from the NginxProxy Custom Resource Definition serverTokens field and the AuthenticationFilter Custom Resource Definition extraAuthArgs field are rendered directly into NGINX configuration templates without sanitization or escaping. An authenticated attacker with permission to create or modify these Custom Resource Definitions may craft values that inject arbitrary NGINX configuration directives. This is a control plane issue; there is no data plane exposure from the vulnerability trigger itself. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-06-17	8.1	CVE-2026-11311
F5--NGINX Gateway Fabric	When NGINX Plus or NGINX Open Source is configured as the data plane for NGINX Gateway Fabric, an injection vulnerability exists in the NGINX configuration generator component of NGINX Gateway Fabric. User-supplied string values from the NginxProxy Custom Resource Definition (CRD) access log format setting are rendered directly into NGINX configuration templates without sanitization or escaping. An authenticated attacker with permission to create or modify these CRDs may craft values that inject arbitrary NGINX configuration directives. This is a control plane issue; there is no data plane exposure from the vulnerability trigger itself. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-06-17	8.1	CVE-2026-50107
F5--NGINX Open Source	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_proxy_v2_module and ngx_http_grpc_module modules. This vulnerability exists when the proxy_http_version to 2 or grpc_pass directives are used to proxy HTTP/2 traffic, the ignore_invalid_headers directive is set to off, and the large_client_header_buffers directive size is larger than 2 megabytes. A remote, unauthenticated attacker, along with conditions beyond their control, could send large headers while creating an upstream request. This may cause a heap-based buffer overflow in the NGINX worker process leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-06-17	8.1	CVE-2026-42055
F5--NGINX Open Source	NGINX Open Source has a vulnerability in the ngx_http_v3_module module. When NGINX Open Source is configured to use the HTTP/3 QUIC module, a remote unauthenticated attacker along with conditions beyond their control can use a specially crafted HTTP/3 session to reopen a QPACK encoder stream. This may cause a Use-after-Free in the NGINX worker process leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout	2026-06-17	8.1	CVE-2026-42530

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Randomization (ASLR) disabled or when the attacker can bypass ASLR. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.			
Faboba--Ultimate Property Listing	Joomla Ultimate Property Listing 1.0.2 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the sf_selectuser_id parameter. Attackers can send GET requests to index.php with the option=com_upl and view=propertylisting parameters to extract sensitive database information including table names and column structures.	2026-06-19	8.2	CVE-2017-20272
FFmpeg--FFmpeg	An out-of-bounds write vulnerability in FFmpeg's libavcodec library, specifically in the MagicYUV decoder, allows denial-of-service and, in some cases, can be exploited for remote code execution. This vulnerability is associated with the file libavcodec/magicyuv.C. This issue affects FFmpeg before version 8.1.2.	2026-06-18	8.8	CVE-2026-8461
fgmacedo--python-statemachine	Python StateMachine versions 3.0.0 before 3.2.0 contains a remote code execution vulnerability that allows attackers to execute arbitrary code by supplying malicious SCXML documents containing crafted `<data expr="...">` attributes evaluated unsafely. The SCXMLProcessor passes attacker-controlled expression strings through a call chain ending in Python's built-in eval() without sandboxing, enabling arbitrary code execution in the context of the hosting process.	2026-06-17	9.8	CVE-2026-47103
Filipe Nasc--RD Station	Improper Control of Generation of Code ('Code Injection') vulnerability in Filipe Nasc RD Station allows Remote Code Inclusion. This issue affects RD Station: from n/a through 5.6.0.	2026-06-16	9.9	CVE-2026-49774
Flipper Code WordPress Development Company--WP Maps	Unauthenticated SQL Injection in WP Maps <= 4.9.1 versions.	2026-06-15	9.3	CVE-2026-39492
Flowise--Flowise	Flowise before 2.1.4 allows configuration to be injected into the Chainflow during execution via the overrideConfig option, supported in both the frontend web integration and the backend Prediction API. Because this feature is enabled by default with no allow-list of permitted variables and relies on vm2 for sandboxing, an attacker can abuse it to achieve remote code execution and sandbox escape, denial of service by crashing the server, server-side request forgery, prompt injection, and server variable and data exfiltration. These issues are self-targeted and do not persist to other users.	2026-06-20	9.8	CVE-2024-58351
Focalpointx--FocalPoint Pro / Free	Joomla! Component FocalPoint Pro/Free 1.2.3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send GET requests to index.php with option=com_focalpoint, view=location, and a crafted id parameter containing SQL commands to extract sensitive database information.	2026-06-19	8.2	CVE-2017-20263
forem--forem	Forem is open source software for building communities. Prior to commit a2ab6d4, a maliciously crafted email address could allow an attacker to bypass domain allowlist or denylist restrictions and gain access to invite-only forem deployments. The issue is patched as of `a2ab6d4`. As a workaround, some SMTP servers and email delivery providers may drop or refuse to send maliciously crafted email addresses.	2026-06-16	8.2	CVE-2026-48780
Fortra--Core Privileged Access Manager (BoKS)	Fortra's Core Privileged Access Manager (BoKS) contains an OS command injection vulnerability in the boks_autoregisterd service. A remote attacker with network access to the service may be able to cause commands to be executed with the privileges of the service during the autoregistration processing.	2026-06-15	9.8	CVE-2026-9862
Fortra--Core Privileged Access Manager (BoKS)	Fortra BoKS Manager contains an OS command injection vulnerability in the client upgrade and patch tooling for legacy tar-based client installations. A malicious or compromised legacy tar-installed client	2026-06-15	7.5	CVE-2026-9863

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	selected for upgrade or patching may be able to cause commands to be executed on the BoKS Master during client version handling.			
Foxit Software Inc.--Foxit AI	When the application executes the JavaScript script embedded in the PDF within the sandbox, it fails to intercept some dangerous interfaces, which allows remote scripts to be loaded, resulting in arbitrary code execution.	2026-06-15	8.6	CVE-2026-12057
fs-code--Booknetic	Unauthenticated Broken Authentication in Booknetic <= 4.8.5 versions.	2026-06-17	8.1	CVE-2026-25439
FunnelKit--Funnel Builder by FunnelKit	Unauthenticated SQL Injection in Funnel Builder by FunnelKit <= 3.15.0.1 versions.	2026-06-15	9.3	CVE-2026-42381
FunnelKit--Funnel Builder by FunnelKit	Unauthenticated Cross Site Scripting (XSS) in Funnel Builder by FunnelKit <= 3.15.0.2 versions.	2026-06-15	7.1	CVE-2026-48966
Gegabyte--My Projects	Joomla! Component My Projects 2.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the VerAyari parameter. Attackers can craft requests to the component endpoint with SQL injection payloads to extract sensitive database information including credentials and system data.	2026-06-19	8.2	CVE-2017-20253
Gegabyte--User Bench	Joomla! Component User Bench 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the userid parameter. Attackers can send GET requests to index.php with the option=com_userbench&view=detail&userid parameter containing SQL injection payloads to extract sensitive database information including credentials and configuration data.	2026-06-19	8.2	CVE-2017-20254
geoserver--org.geoserver.extensions:gs-db2	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to version 2.27.0 of the GeoServer DB2 DataStore Extension, an administrator can perform a JNDI attack through specially crafted DB2 jdbc url leading to Remote Code Execution (RCE). Version 2.27.0 fixes the issue.	2026-06-18	7.2	CVE-2025-27511
geoserver--org.geoserver.web:gs-web-app	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.26.4 and 2.27.3, a vulnerability exists that allows an authenticated administrator with access to GeoServer's security system to pass arbitrary file names to the Master Password Dump web page and create files containing the master password in plaintext. The provided file name must be an absolute path to the target file, the target file can not already exist and all parent directories must already exist. Versions 2.26.4 and 2.27.3 contain a fix. GeoServer installations where the web interface is either disabled or completely removed are not affected since the vulnerability exists in one of the web pages.	2026-06-18	7.2	CVE-2025-52465
gitroomhq--postiz-app	Postiz is an AI social media scheduling tool. In versions prior to 2.21.8, the Skool integration callback signed an attacker-controlled JSON blob into a session-shape JWT using the application's JWT_SECRET, and the auth middleware trusted every claim in that JWT without re-resolving the user from the database. Any authenticated Postiz user could forge a SUPERADMIN session and impersonate arbitrary organizations. This allowed Full Access to the following: all parts of Postiz, including users registered to the specific instance and the ability to post in the name of the victim's social media channels added to that Postiz instance. This issue has been fixed in version 2.21.8.	2026-06-16	9.9	CVE-2026-48781
Glen Don Mongaya--Drag and Drop Multiple File Upload Contact Form 7	Unauthenticated Cross Site Scripting (XSS) in Drag and Drop Multiple File Upload - Contact Form 7 <= 1.3.9.7 versions.	2026-06-15	7.1	CVE-2026-49055
Government Accountability	The U.S. Government Accountability Office (GAO) Electronic Protest Docketing System (EPDS) and Civilian Board of Contract Appeals (CBCA)	2026-06-18	9.8	CVE-2026-54103

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Office--Electronic Protest Docketing System (EPDS)	Electronic Docketing System (EDS) does not authenticate password change requests to the '/update-profile/N' API endpoint. A remote, unauthenticated attacker could change an arbitrary user's password.			
Government Accountability Office--Electronic Protest Docketing System (EPDS)	The U.S. Government Accountability Office (GAO) Electronic Protest Docketing System (EPDS) and Civilian Board of Contract Appeals (CBCA) Electronic Docketing System (EDS) trusts client-provided values for the 'epds_role_id' parameter without verification, allowing a remote, authenticated attacker to escalate their own privileges.	2026-06-18	8.8	CVE-2026-54104
Groundhogg--Groundhogg	Sales Representative Arbitrary File Deletion in Groundhogg <= 4.4 versions.	2026-06-15	7.7	CVE-2026-40727
Groundhogg--HollerBox	Unauthenticated Cross Site Scripting (XSS) in HollerBox <= 2.3.10.1 versions.	2026-06-15	7.1	CVE-2026-48885
Hakan Ozevin--WP BASE Booking	Unauthenticated Privilege Escalation in WP BASE Booking <= 5.9.0 versions.	2026-06-15	8.1	CVE-2026-39587
Happyforms--Happyforms	Unauthenticated PHP Object Injection in Happyforms <= 1.26.13 versions.	2026-06-15	9.8	CVE-2026-49768
haproxy--haproxy	HAProxy through 3.4.0, fixed in commit 5985276, contains an integer overflow vulnerability in the fcgi_conn structure's drl field that allows buffer misparse as new FCGL record headers. When contentLength is 65535 and paddingLength is 1 or more, the drl field wraps to 0, causing incorrect record consumption and allowing malicious FastCGI backends to desynchronize the FCGL framing parser, potentially causing request routing errors, response smuggling, or memory safety issues.	2026-06-18	7.5	CVE-2026-55203
haproxy--haproxy	HAProxy through 3.4.0, fixed in commit 9a6d1fe, contains a null pointer dereference vulnerability in hpack_dht_insert() within src/hpack-tbl.c that fails to validate the return value of hpack_dht_defrag() when the memory pool is exhausted. An attacker can trigger HPACK dynamic table insertions under memory pressure to dereference a NULL pointer and crash HAProxy worker processes, causing denial of service.	2026-06-18	7.5	CVE-2026-55204
harttle--liquidjs	LiquidJS is a Shopify/GitHub Pages compatible template engine written in pure JavaScript. In versions 10.25.7 and below, the date filter's strftime implementation parses width specifiers like %99999999d and forwards the captured width unchecked into pad()/padStart(), leading to memory and render limit bypass. In src/util/underscore.ts, the pad loop performs unbounded string concatenation without consulting the Context's memoryLimit or renderLimit, so a single small template ({{ x date: '%5000000d' }}) produces megabytes of output and unbounded CPU. The memoryLimit and renderLimit options the docs (src/liquid-options.ts:87-92) advertise as DoS controls - and which the docstring explicitly mentions for strftime - are entirely bypassed. Exploitation can cause large memory allocations, high CPU usage, or OOM crashes per render. This issue has been fixed in version 10.26.0.	2026-06-17	7.5	CVE-2026-45357
harttle--liquidjs	LiquidJS is a Shopify/GitHub Pages compatible template engine written in pure JavaScript. In versions 10.25.7 and below, the built-in strip_html filter uses a regex containing four flawed lazy-quantified alternatives, leading to ReDoS via quadratic backtracking. When the input contains many <script, <style, or <!-- opener tokens without matching closers, the V8 regex engine performs O(N^2) backtracking, blocking the Node.js event loop. A single ~350 KB request ('<script'.repeat(50000)) stalls the process for ~10 seconds; cost grows quadratically with input size. The default memoryLimit: Infinity does not bound regex CPU, and even when configured strip_html only charges str.length to the limit - the regex itself runs unbounded. A single unauthenticated request containing crafted untrusted input can cause severe event-loop blocking and CPU amplification that saturates Node.js workers while bypassing memoryLimit protections. This issue has been fixed in version 10.26.0.	2026-06-17	7.5	CVE-2026-45617

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Henryschorrad--Bridge	Joomla! Component PHP-Bridge 1.2.3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send GET requests to index.php with option=com_phpbridge&view=phpview parameters and inject SQL code in the id parameter to extract database information including table and column names.	2026-06-19	8.2	CVE-2017-20275
hermes-webui--hermes-webui	Hermes WebUI before 0.51.409 contains an authentication bypass vulnerability in passkey registration endpoints that allows unauthenticated remote attackers to register arbitrary passkeys. When HERMES_WEBUI_PASSKEY=1 is enabled with no existing credentials, POST /api/auth/passkey/register/options and POST /api/auth/passkey/register endpoints are accessible without authentication, allowing attackers to claim the first passkey and gain permanent administrative control.	2026-06-17	9.1	CVE-2026-55196
hippooo--Hippoo Mobile App for WooCommerce	Unauthenticated Broken Access Control in Hippoo Mobile App for WooCommerce <= 1.9.5 versions.	2026-06-15	8.2	CVE-2026-49065
Hitachi--Hitachi Virtual Storage Platform E990, E1090, E1090H	DoS Vulnerability in 10G iSCSI Interface of Hitachi Virtual Storage Platform. This issue affects Hitachi Virtual Storage Platform E990, E1090, E1090H: before DKCMAIN Ver.93-07-21-80/00-05, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-07-01-80/00-07, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-06-82-80/00-06, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-06-63-80/00-04, CHB(iSCSI) Ver.88-01-02-04; Hitachi Virtual Storage Platform E390, E590, E790, E390H, E590H, E790H: before DKCMAIN Ver.93-07-21-x0/00-05, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-07-01-x0/00-07, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-06-82-x0/00-06, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-06-63-x0/00-04, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-07-24-x0/00-02, CHB(iSCSI) Ver.88-01-02-04, before DKCMAIN Ver.93-07-02-x0/00-02, CHB(iSCSI) Ver.88-01-02-04; Hitachi Virtual Storage Platform G130, G150, G350, G370, G700, G900, F350, F370, F700, F900: before DKCMAIN Ver.88-08-10-x0/00-05, CHB(iSCSI) Ver.88-01-02-04; Hitachi Virtual Storage Platform G100, G200, G400, G600, G800, F400, F600, F800: before DKCMAIN Ver.83-06-20-x0/00-05, CHB(iSCSI) Ver.83-01-01-29; Hitachi Virtual Storage Platform VX8, 5100, 5500, 5100H, 5500H, 5200, 5600, 5200H, 5600H: before DKCMAIN Ver.90-09-01-00/01-01, CHB(iSCSI) Ver.90-01-01-07, before DKCMAIN Ver.90-08-83-00/01-01, CHB(iSCSI) Ver.90-01-01-07, before DKCMAIN Ver.90-08-63-00/01-01, CHB(iSCSI) Ver.90-01-01-07; Hitachi Virtual Storage Platform VX7, G1000, G1500, F1500: before DKCMAIN Ver.80-06-93-00/00-04, ISFC Ver.80-01-17.	2026-06-19	8.6	CVE-2025-7737
HKUDS--nanobot	nanobot is a personal AI assistant. In versions 0.1.5.post3 and prior, the WhatsApp bridge in bridge/src/whatsapp.ts constructs a filesystem path using the fileName field from an incoming WhatsApp document message without sanitization. The WhatsApp bridge downloads media attachments and writes them to disk using a filename derived from the sender's message via documentMessage.fileName, which is concatenated with a prefix and its raw value is passed directly to path.join(mediaDir, outFilename). Node.js path.join resolves .. components, allowing an attacker to escape the intended media/ directory by sending a document with a crafted fileName such as ../../.ssh/authorized_keys. Because the attacker also controls the file content (the downloaded buffer), this is a write-anywhere primitive - both path and content are attacker-controlled. A fix for this issue is planned for version 0.1.5.post4.	2026-06-18	8.7	CVE-2026-48716
https://wprevie.wslider.com/ --WP Review Slider Pro	The WP Review Slider Pro plugin for WordPress is vulnerable to Arbitrary File Deletion in versions up to and including 12.6.8. This is due to missing authorization checks on the wpfb_hide_review and wprp_save_review_admin AJAX handlers combined with insufficient path validation in the wpfb_hidereview_ajax() function, which uses strpos() to	2026-06-16	8.1	CVE-2026-8442

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	check that a stored media URL starts with the expected prefix but fails to sanitize path traversal sequences in the remaining relative path before passing it to unlink(). This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary files on the affected site's server which may make remote code execution possible.			
https://wprevie.wslider[.]com/--WP-Review-Slider-Pro	The WP Review Slider Pro plugin for WordPress is vulnerable to SQL Injection via the 'types' and 'slocations' parameters of the wppro_get_overall_chart_data AJAX action in versions up to, and including, 12.6.8. This is due to the use of stripslashes() on user-supplied JSON strings prior to json_decode(), which removes the escaping applied by WordPress's wp_magic_quotes; the resulting decoded array values are then concatenated directly into SQL WHERE clauses without parameterization, and the constructed query is executed via \$wpdb->get_results() without \$wpdb->prepare(). This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The handler also returns the executed SQL string in its JSON response, which simplifies oracle construction for blind exploitation.	2026-06-16	8.8	CVE-2026-8443
https://wprevie.wslider[.]com/--WP-Review-Slider-Pro	The WP Review Slider Pro plugin for WordPress is vulnerable to SQL Injection via the 'curselrevs[]' parameter of the wpfb_find_reviews AJAX action in versions up to, and including, 12.6.8. This is due to the handler reading \$_POST['curselrevs'] raw with no sanitization or type casting, then concatenating each array element directly into a `WHERE id IN ( ... )` clause without quoting and executing via \$wpdb->get_results() without \$wpdb->prepare(). This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-06-16	8.8	CVE-2026-8444
Husain--HB Audio Gallery Lite	WordPress Plugin HB Audio Gallery Lite 1.0.0 contains a path traversal vulnerability that allows unauthenticated attackers to download arbitrary files by manipulating the file_path parameter. Attackers can send requests to the audio-download.php endpoint with directory traversal sequences to access sensitive files like wp-config.php outside the intended gallery directory.	2026-06-15	7.5	CVE-2016-20081
i18next--i18next-fs-backend	Versions prior to 2.6.6 are vulnerable to prototype pollution via crafted missing-key strings when used to persist missing translation keys (e.g. via i18next-http-middleware's missingKeyHandler exposed to untrusted input). Backend.writeFile() splits each queued missing-key string on the configured keySeparator (default .) before calling the internal setPath() walker. The walker (getLastOfPath in lib/utls.js) did not guard against unsafe segments, so a key like "__proto__.polluted" was split into ["__proto__", "polluted"] and walked straight into Object.prototype, allowing an attacker to write arbitrary properties onto the global object prototype. Depending on the host application, polluted prototype properties may cause crashes, corrupted translation behaviour, configuration poisoning, or bypasses of property-based security checks. Applications are affected only if the missingKeyHandler (or another route that forwards untrusted request bodies to i18next.t(..., { ... }) with saveMissing: true) is reachable by untrusted users and the default behaviour of splitting missing-key strings on keySeparator is in use (i.e. keySeparator is not false). Apps that do not expose missing-key persistence to untrusted input are not directly affected through this attack path. This issue has been fixed in version 2.6.6. If developers using the library are unable to upgrade immediately, they should take the following precautions: do not expose i18next-http-middleware's missingKeyHandler to untrusted users (mount it behind authentication, or remove the route), disable missing-key persistence (saveMissing: false, or no backend.create implementation) when accepting writes from untrusted input, and set	2026-06-15	9.1	CVE-2026-48713

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	keySeparator: false in their i18next options to disable backend key splitting (note: this also disables nested translation keys).			
i18next--i18next-http-middleware	i18next-http-middleware is a middleware to be used with Node.js web frameworks like express or Fastify and also for Deno. In versions prior to 3.9.7, the missingKeyHandler blocked the literal request-body keys __proto__, constructor, and prototype (added in 3.9.3, see GHSA-5fgg-jcpf-8jjw), but did not reject dotted variants such as "__proto__.polluted". Downstream backends that split the missing-key string on a configured keySeparator (notably i18next-fs-backend 2.6.5) hand these keys to an unguarded setPath() walker that writes to Object.prototype. Applications that expose missingKeyHandler to untrusted input AND use i18next-fs-backend 2.6.5 are directly exploitable for remote prototype pollution. Other downstream backends that split the missing-key string the same way may be similarly affected. Depending on the host application, polluted prototype properties may cause crashes, corrupted translation behaviour, configuration poisoning, or bypasses of property-based security checks. This issue has been fixed in version 3.9.7. If developers cannot upgrade immediately, they should do the following: do not expose missingKeyHandler to untrusted users (mount it behind authentication, or remove the route), add a request-body filter ahead of the handler that rejects any top-level key containing __proto__, constructor, or prototype after splitting on their configured keySeparator, and disable missing-key persistence (saveMissing: false) when accepting writes from untrusted input.	2026-06-15	9.1	CVE-2026-48714
iba--ibaPDA	A remote, unauthenticated attacker may exploit a deserialization of untrusted data vulnerability in ibaPDA or ibaDatCoordinator to gain full access to the affected systems.	2026-06-18	9.8	CVE-2026-8024
IDPay--IDPay Payment Gateway for Woocommerce	Unauthenticated Sensitive Data Exposure in IDPay Payment Gateway for Woocommerce <= 2.2.5 versions.	2026-06-15	7.5	CVE-2026-34891
IM-Magic--Partition Resizer	A weakness has been identified in IM-Magic Partition Resizer up to 7.9.0. This affects an unknown function in the library MDA_NTDRV.sys of the component Kernel Driver. This manipulation causes improper access controls. The attack requires local access. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	7.8	CVE-2026-12784
impleCode--eCommerce Product Catalog	Unauthenticated SQL Injection in eCommerce Product Catalog <= 3.5.5 versions.	2026-06-15	9.3	CVE-2026-52693
Inisev--Backup Migration	Unauthenticated Sensitive Data Exposure in Backup Migration <= 2.1.1 versions.	2026-06-15	7.5	CVE-2026-39480
Iperiusremote--Iperius Remote	Iperius Remote 1.7.0 contains an unquoted service path vulnerability that allows local users to execute arbitrary code with SYSTEM privileges by exploiting the service installation path. When installed from directories containing spaces, attackers can place malicious executables in the path to be executed with elevated privileges during service startup or system reboot.	2026-06-19	7.8	CVE-2016-20089
IT Path Solutions--Contact Form to Any API	Unauthenticated Cross Site Scripting (XSS) in Contact Form to Any API <= 3.0.3 versions.	2026-06-15	7.1	CVE-2026-39449
Jacob N. Breetvelt--WP Photo Album Plus	Unauthenticated SQL Injection in WP Photo Album Plus <= 9.1.08.001 versions.	2026-06-15	9.3	CVE-2026-39511
JetBrains--GoLand	In JetBrains GoLand before 2026.1.3 remote code execution was possible via untrusted project configuration	2026-06-19	7.1	CVE-2026-53915

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
JetBrains--Hub	In JetBrains Hub before 2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429 authentication bypass via direct database access leading to administrative access was possible	2026-06-19	10	CVE-2026-50242
JetBrains--Hub	In JetBrains Hub before 2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429 account takeover via predictable restore codes was possible	2026-06-19	9.8	CVE-2026-56141
JetBrains--Hub	In JetBrains Hub before 2026.1.13757, 2025.3.148033, 2025.2.148048, 2025.1.148120, 2024.3.148430, 2024.2.148429 privilege escalation by attaching authentication details to accounts was possible	2026-06-19	9.6	CVE-2026-56142
Jetimpex Inc.--JetBlog	Unauthenticated Sensitive Data Exposure in JetBlog <= 2.4.8 versions.	2026-06-17	7.5	CVE-2026-52696
Jetimpex Inc.--JetEngine	Contributor PHP Object Injection in JetEngine <= 3.8.9.1 versions.	2026-06-17	9.8	CVE-2026-49075
Jetimpex Inc.--JetEngine	Unauthenticated SQL Injection in JetEngine <= 3.8.9.1 versions.	2026-06-17	9.3	CVE-2026-49076
Jetimpex Inc.--JetEngine	Unauthenticated SQL Injection in JetEngine < 3.8.9.1 versions.	2026-06-17	9.3	CVE-2026-49084
Jetimpex Inc.--JetEngine	Unauthenticated PHP Object Injection in JetEngine <= 3.8.10 versions.	2026-06-17	9.8	CVE-2026-52706
Jetimpex Inc.--JetEngine	Unauthenticated SQL Injection in JetEngine <= 3.8.10.1 versions.	2026-06-17	9.3	CVE-2026-54187
Jetimpex Inc.--JetEngine	Unauthenticated Cross Site Scripting (XSS) in JetEngine <= 3.8.9.1 versions.	2026-06-17	7.1	CVE-2026-49074
Jetimpex Inc.--JetEngine	Unauthenticated Cross Site Scripting (XSS) in JetEngine <= 3.8.10 versions.	2026-06-17	7.1	CVE-2026-54188
Jetimpex Inc.--JetEngine	Unauthenticated Cross Site Scripting (XSS) in JetEngine <= 3.8.10 versions.	2026-06-17	7.1	CVE-2026-54189
Jetimpex Inc.--JetSearch	Unauthenticated SQL Injection in JetSearch <= 3.5.17 versions.	2026-06-17	9.3	CVE-2026-49079
Jetimpex Inc.--JetSmartFilters	Unauthenticated SQL Injection in JetSmartFilters <= 3.8.1 versions.	2026-06-17	9.3	CVE-2026-48875
Jetmonsters--JetFormBuilder	Unauthenticated Cross Site Scripting (XSS) in JetFormBuilder <= 3.6.0.1 versions.	2026-06-17	7.1	CVE-2026-54195
JExtensions Store--GPTranslate Multilingual AI Translation for WordPress: Automatically Translate Websites	Unauthenticated SQL Injection in GPTranslate - Multilingual AI Translation for WordPress: Automatically Translate Websites <= 2.32.6 versions.	2026-06-15	9.3	CVE-2026-49776
jkdevstudio--Qreatix	Unauthenticated Cross Site Scripting (XSS) in Qreatix <= 1.9.4 versions.	2026-06-16	7.1	CVE-2025-69104
Jobster Marketplace--WPJobster	Unauthenticated SQL Injection in WPJobster <= 6.3.5 versions.	2026-06-17	9.3	CVE-2026-22340
Jobster Marketplace--WPJobster	Unauthenticated Cross Site Scripting (XSS) in WPJobster <= 6.3.5 versions.	2026-06-17	7.1	CVE-2026-22339
Joombooking--JB Visa	Joomla! Component JB Visa 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the visatype parameter. Attackers can send GET requests to index.php with the option=com_bookpro and view=popup parameters, injecting SQL commands in the visatype parameter to extract sensitive database information including credentials and table contents.	2026-06-19	8.2	CVE-2017-20255

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Joomboost--JoomCRM	Joomla! Component JoomCRM 1.1.1 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the deal_id parameter. Attackers can send GET requests to index.php with option=com_joomcrm&view=contacts and inject SQL code in the deal_id parameter to extract sensitive database information including table names and schemas.	2026-06-19	7.1	CVE-2019-25761
Joomboost--Joomla JoomRecipe	Joomla JoomRecipe 1.0.4 component contains a blind SQL injection vulnerability in the search_author parameter on the search results page. Attackers can inject SQL code through POST requests to the search endpoint to extract database information using boolean-based blind SQL injection techniques.	2026-06-19	8.2	CVE-2017-20277
Joomboost--JoomProject	Joomla! Component JoomProject 1.1.3.2 contains an information disclosure vulnerability that allows unauthenticated attackers to access sensitive user data by exploiting the projects endpoint. Attackers can send requests to index.php with option=com_jpprojects&view=projects&tmpl=component&format=json parameters to retrieve user IDs, names, and email addresses in JSON format.	2026-06-19	7.5	CVE-2019-25762
Joomboost--JoomRecipe	Joomla Component JoomRecipe 1.0.3 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the category parameter. Attackers can send GET requests to the all-recipes endpoint with malicious SQL payloads in the category path segment to extract sensitive database information.	2026-06-19	8.2	CVE-2017-20278
Joomlaboat--Extra Search	Joomla! Component Extra Search 2.2.8 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the establename parameter. Attackers can send GET requests to index.php with the option=com_extrasearch parameter and malicious SQL in the establename field to extract sensitive database information.	2026-06-19	8.2	CVE-2017-20281
Joomlashack--OSDownloads	Joomla OSDownloads 1.7.4 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send GET requests to index.php with option=com_osdownloads&view=item&id=[SQL] to extract sensitive database information including credentials and configuration data.	2026-06-19	8.2	CVE-2017-20259
Joomlashowroom--Event Registration Pro Calendar	Joomla Event Registration Pro Calendar 4.1.3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the id parameter. Attackers can send GET requests to index.php with option=com_registrationpro&view=category&id parameter containing SQL injection payloads to extract sensitive database information.	2026-06-19	8.2	CVE-2017-20273
Joomlathat--Calendar Planner	Joomla! Component Calendar Planner 1.0.1 contains an SQL injection vulnerability that allows unauthenticated attackers to inject SQL commands through the category_id parameter. Attackers can send GET requests to the events view with malicious SQL code in the category_id parameter to extract sensitive database information.	2026-06-19	8.2	CVE-2017-20267
Joomplace--Quiz Deluxe	Joomla! Component Quiz Deluxe 3.7.4 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL commands through the ajaxaction.flag_question task. Attackers can inject malicious SQL code via the stu_quiz_id or flag_quest parameters to manipulate database queries and extract sensitive information.	2026-06-19	8.2	CVE-2017-20257
Joomplace--Survey Force Deluxe	Joomla Survey Force Deluxe 3.2.4 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the invite parameter. Attackers can send GET requests to the component with crafted SQL payloads in the invite parameter to extract sensitive database information.	2026-06-19	8.2	CVE-2017-20256

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Joomshaper--SP Movie Database	Joomla SP Movie Database 1.3 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the searchword parameter. Attackers can send GET requests to the searchresults view with crafted SQL payloads in the searchword parameter to extract sensitive database information.	2026-06-19	8.2	CVE-2017-20266
Joomunited--WP Media folder Addon	Unauthenticated Arbitrary File Download in WP Media folder Addon <= 4.0.1 versions.	2026-06-17	7.5	CVE-2026-9690
Jose Conti--Redsys for WooCommerce Light	Unauthenticated Broken Access Control in Redsys for WooCommerce Light <= 7.0.0 versions.	2026-06-15	7.5	CVE-2026-40741
Jovancoding--Network-AI	Network-AI is a TypeScript/Node.js multi-agent orchestrator. In versions 5.7.1 and earlier, the MCP SSE server allows unauthenticated cross-origin MCP tool invocation due to an empty default secret. This issue was partially addressed by CVE-2026-46701 in version 5.4.5 by closing the CORS flaw (with Access-Control-Allow-Origin now set only for localhost origins), but the empty-default-secret flaw described in the title remained: the SSE MCP server still defaulted to an empty secret, <code>_isAuthorized()</code> still returned true when the secret was empty, and a non-loopback bind only produced a warning. As a result, the server still ran fully unauthenticated by default. Any non-browser caller (for example, curl, SSRF, or a 0.0.0.0 bind) could invoke all 22 MCP tools (<code>config_set</code> , <code>agent_spawn</code> , <code>blackboard_write</code> , <code>token_*</code>) with no credentials. This issue was fixed in version 5.7.2.	2026-06-17	9.1	CVE-2026-48814
Jthemes--Genemy	Subscriber Privilege Escalation in Genemy <= 1.6.6 versions.	2026-06-17	8.8	CVE-2025-69138
JTL Software--JTL Shop	JTL Shop versions 5.2.0 through 5.7.1 contains a server-side template injection vulnerability that allows unauthenticated attackers to inject malicious template syntax due to unsanitized user-supplied input passed to the Smarty template engine. Attackers can exploit this flaw to read sensitive server-side values such as database credentials and encryption keys, and on versions 5.4.0 through 5.7.1, leverage registered Smarty modifiers including <code>unserialize</code> and <code>file_get_contents</code> to write a webshell to the web root and execute arbitrary commands as the web server user.	2026-06-18	9.8	CVE-2026-54390
jwstthemes--AI Lab	Unauthenticated PHP Object Injection in AI Lab < 5.4.2 versions.	2026-06-17	9.8	CVE-2026-42380
kilbot--WooCommerce POS	Unauthenticated Broken Access Control in WooCommerce POS <= 1.8.14 versions.	2026-06-16	7.5	CVE-2026-52711
King-products--LMS King Professional	Joomla LMS King Professional 3.2.4.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the <code>cp_id</code> parameter. Attackers can send GET requests to <code>index.php</code> with the <code>option=com_lmsking</code> , <code>view=lmsking</code> , <code>layout=learningpath</code> , and <code>task=learningPath</code> parameters to extract sensitive database information.	2026-06-19	8.2	CVE-2017-20274
Kludex--starlette	Starlette is a lightweight ASGI framework/toolkit. In versions 1.0.1 and earlier, StaticFiles on Windows is vulnerable to SSRF. An UNC path such as <code>\\attacker.com\\share</code> can cause <code>os.path.realpath</code> to initiate an outbound SMB connection before the path is rejected, exposing the service account's NTLMv2 credentials for offline cracking or relay even though the HTTP response is only a 404. The issue affects default <code>follow_symlink=False</code> deployments, including frameworks built on Starlette such as FastAPI; POSIX systems and <code>follow_symlink=True</code> are unaffected. The issue is fixed in 1.1.0.	2026-06-17	7.5	CVE-2026-48818
Knit Pay--Knit Pay	Unauthenticated Broken Access Control in Knit Pay <= 9.4.0.0 versions.	2026-06-15	7.5	CVE-2026-49070

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Kodezen LLC--Academy LMS Pro	Unrestricted Upload of File with Dangerous Type vulnerability in Kodezen LLC Academy LMS Pro allows Upload a Web Shell to a Web Server. This issue affects Academy LMS Pro: from n/a before 3.5.2.	2026-06-16	8	CVE-2026-39598
Kriesi--Enfold	Unauthenticated Cross Site Scripting (XSS) in Enfold <= 7.1.4 versions.	2026-06-16	7.1	CVE-2026-48869
LatePoint--LatePoint	Contributor Privilege Escalation in LatePoint <= 5.5.1 versions.	2026-06-15	7.5	CVE-2026-49083
latepoint--LatePoint Calendar Booking Plugin for Appointments and Events	The LatePoint - Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Privilege Escalation to Administrator in versions up to, and including, 5.5.1. The plugin chains three independent flaws that together allow an authenticated Agent (Agent+) to overwrite a WordPress Administrator's password without ever invoking an Administrator-only API. This makes it possible for authenticated attackers, with Agent access and above, to elevate their privileges to Administrator.	2026-06-16	7.5	CVE-2026-8176
leejet--stable-diffusion.cpp	stable-diffusion.cpp is a pure C/C++ library for running diffusion model (Stable Diffusion, Flux, Wan, Qwen Image, Z-Image, and more) inference. In versions prior to master-584-0a7ae07, the pickle .ckpt parser in src/model.cpp contained a heap buffer overflow vulnerability in the BINUNICODE opcode handler. The issue was caused by sign confusion on the opcode length field. A crafted .ckpt file could trigger memcpy with a very large length derived from a negative signed value, causing immediate heap corruption. The issue has been resolved in version master-584-0a7ae07. If developers are unable to immediately update their applications they can work around this issue by only loading .ckpt checkpoint files from trusted sources and preferring trusted model sources and safer formats such as .safetensors where possible.	2026-06-16	7.8	CVE-2026-47747
leejet--stable-diffusion.cpp	stable-diffusion.cpp is a pure C/C++ library for running diffusion model (Stable Diffusion, Flux, Wan, Qwen Image, Z-Image, and more) inference. Versions prior to master-584-0a7ae07 are vulnerable to heap buffer overflow in SHORT_BINUNICODE parsing for PyTorch checkpoint files. The pickle .ckpt parser in src/model.cpp contained a heap buffer overflow vulnerability in the SHORT_BINUNICODE opcode handler. The issue was caused by sign confusion on the opcode length field. A crafted .ckpt file could trigger memcpy with a very large length derived from a negative signed value, causing immediate heap corruption. Any application using affected stable-diffusion.cpp releases to load untrusted .ckpt model files could be vulnerable. A malicious checkpoint file could cause heap corruption through memcpy with an attacker-controlled length. This may lead to process crash and could potentially be leveraged for code execution depending on heap layout. The attack requires the victim or application to load a .ckpt file from an untrusted source, such as a downloaded model from a model sharing site. The issue has been resolved in version master-584-0a7ae07. If developers are unable to immediately update their applications they can work around this issue by not loading .ckpt checkpoint files from untrusted sources, and referring to trusted model sources and safer formats such as .safetensors where possible.	2026-06-16	7.8	CVE-2026-47749
leejet--stable-diffusion.cpp	stable-diffusion.cpp is a pure C/C++ library for running diffusion model (Stable Diffusion, Flux, Wan, Qwen Image, Z-Image, and more) inference. In versions prior to master-584-0a7ae07, the pickle .ckpt parser in src/model.cpp contained a heap buffer overflow vulnerability in the GLOBAL opcode handler. The issue was caused by missing validation when searching for newline-delimited fields. A crafted .ckpt file without the expected newline could cause the parser to use -1 as a copy length, resulting in immediate heap corruption. The attack requires the victim or application to load a .ckpt file from an untrusted source, such as a downloaded model from a model sharing site. The issue has been resolved in version master-584-0a7ae07. If developers are unable to immediately update their applications they can work around this issue by following these instructions: do not load .ckpt checkpoint files from untrusted	2026-06-16	7.8	CVE-2026-47750

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sources, and prefer trusted model sources and safer formats such as .safetensors where possible.			
libssh2--libssh2	libssh2 through 1.11.1, fixed in commit 7acf3df contains an out-of-bounds write vulnerability in ssh2_transport_read() that fails to enforce upper bounds on packet_length field. Remote attackers can send crafted SSH packets with excessively large packet_length values to corrupt heap memory and achieve remote code execution.	2026-06-17	8.1	CVE-2026-55200
Liquid Web / StellarWP--GiveWP	Unauthenticated Cross Site Scripting (XSS) in GiveWP <= 4.14.2 versions.	2026-06-15	7.1	CVE-2026-34900
Liquid Web / StellarWP--The Events Calendar	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Liquid Web / StellarWP The Events Calendar allows Blind SQL Injection. This issue affects The Events Calendar: from 6.15.12 through 6.16.2.	2026-06-16	9.3	CVE-2026-49772
LoginPress--LoginPress Pro	Unauthenticated Privilege Escalation in LoginPress Pro <= 6.2.2 versions.	2026-06-17	9.8	CVE-2026-49058
Magepeople inc.--WpEvently	Unauthenticated Other Vulnerability Type in WpEvently <= 5.3.3 versions.	2026-06-15	7.5	CVE-2026-45441
Magepeople inc.--WpTravelly	Unauthenticated Bypass Vulnerability in WpTravelly <= 2.1.7 versions.	2026-06-15	7.5	CVE-2026-27089
Malwarebytes--Malwarebytes	Malwarebytes 4.5 contains an unquoted service path vulnerability in the MBAMService executable that allows local attackers to escalate privileges by injecting malicious code into the system root path. Attackers can place executable files in unquoted path directories that execute with LocalSystem privileges during service startup or system reboot.	2026-06-19	7.8	CVE-2022-50971
Mamunur Rashid--Classified Listing	Unauthenticated Cross Site Scripting (XSS) in Classified Listing <= 5.3.8 versions.	2026-06-15	7.1	CVE-2026-42658
ManageWP--ManageWP Worker	Unauthenticated Cross Site Scripting (XSS) in ManageWP Worker <= 4.9.31 versions.	2026-06-15	7.1	CVE-2026-39463
MantraBrain--Easy Invoice	Unauthenticated Remote Code Execution (RCE) in Easy Invoice <= 2.1.19 versions.	2026-06-15	10	CVE-2026-48836
mariovalney--CF7 to Webhook	The CF7 to Webhook plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 5.0.0 via the pull_the_trigger. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. Exploitation requires that the admin-configured webhook URL contains a Contact Form 7 field placeholder in the host segment of the URL, and that the affected form is publicly accessible.	2026-06-18	7.2	CVE-2026-11395
markbeljaars--iRobots.txt SEO	Unauthenticated Cross Site Scripting (XSS) in iRobots.txt SEO <= 1.1.2 versions.	2026-06-15	7.1	CVE-2025-68840
mastodon--mastodon	Mastodon is a free, open-source social network server based on ActivityPub. In versions there is a missing condition in the check if remote accounts consented to be featured in a remote Collection could lead to attackers bypassing the check and faking consent. An attacker could forge the FeatureAuthorization object that is used to verify consent to be featured in a Collection and thus make it appear as if an account is allowed to be in a Collection when it actually is not. While the FeatureAuthorization must reside on the same domain as the object it is for, a check is missing to make sure said object is actually the same as in the Collection item. This allows an attacker to forge the authorization. Mastodon servers are affected only if running the main branch or nightly builds who have opted into testing the experimental "Collections" feature by setting the environment variable EXPERIMENTAL_FEATURES to a value including collections. This has been patched in version 4.6.0-beta.1.	2026-06-15	7.5	CVE-2026-47777

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Matrix42-- Matrix42 Remote Control Host	Matrix42 Remote Control Host 3.20.0031 contains an unquoted service path vulnerability in the FastViewerRemoteService and FastViewerRemoteProxy services that allows local users to execute arbitrary code with SYSTEM privileges. Attackers can place a malicious executable in the Program Files directory with a crafted name to be executed by the service during startup, gaining elevated privileges.	2026-06-19	7.8	CVE-2016-20095
mattkaye-- Answer My Question	Answer My Question 1.3 plugin for WordPress contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'id' POST parameter. Attackers can submit crafted SQL statements to the modal.php endpoint to extract sensitive database information including WordPress terms and configuration data.	2026-06-15	8.2	CVE-2016-20073
Melapress--WP Activity Log	Unauthenticated PHP Object Injection in WP Activity Log <= 5.6.3.1 versions.	2026-06-17	9.8	CVE-2026-54806
melhorenvio-- Melhor Envio	Subscriber Broken Authentication in Melhor Envio <= 2.16.3 versions.	2026-06-17	7.6	CVE-2026-54804
Meow Apps--AI Engine	Editor Privilege Escalation in AI Engine <= 3.4.9 versions.	2026-06-15	7.2	CVE-2026-27407
Metagauss-- RegistrationMagic	Unauthenticated Broken Authentication in RegistrationMagic <= 6.0.8.6 versions.	2026-06-15	9.8	CVE-2026-49764
metaphorcreations--Post Duplicator	Contributor PHP Object Injection in Post Duplicator <= 3.0.10 versions.	2026-06-15	8.8	CVE-2026-39474
MetaSlider-- Responsive Slider by MetaSlider	Editor Remote Code Execution (RCE) in Responsive Slider by MetaSlider <= 3.106.0 versions.	2026-06-15	9.1	CVE-2026-39465
MIA Technology Inc.--Pizzy Library	Improper neutralization of formula elements in a CSV file vulnerability in MIA Technology Inc. Pizzy Library allows Code Injection. This issue affects Pizzy Library: from 1.0.0.26250 before 1.3.9.26250.	2026-06-15	8.8	CVE-2026-5242
MIA Technology Inc.--Pizzy Library	Improper Access Control, Missing Authorization vulnerability in MIA Technology Inc. Pizzy Library allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Pizzy Library: from 1.0.0.26250 before 1.3.9.26250.	2026-06-15	7.1	CVE-2026-5230
MIA Technology Inc.--Pizzy Library	Improper Control of Interaction Frequency vulnerability in MIA Technology Inc. Pizzy Library allows Flooding. This issue affects Pizzy Library: from 1.0.0.26250 before 1.3.9.26250.	2026-06-15	7.1	CVE-2026-5233
Microsoft--Azure Active Directory	Improper authentication in Azure Active Directory allows an unauthorized attacker to elevate privileges over a network.	2026-06-19	10	CVE-2026-45480
Microsoft--Azure AI Bot Service	Improper authentication in Azure Bot Service allows an authorized attacker to elevate privileges over a network.	2026-06-18	7.7	CVE-2026-32174
Microsoft--Azure Synapse	Execution with unnecessary privileges in Azure Synapse allows an authorized attacker to elevate privileges over a network.	2026-06-19	9.9	CVE-2026-48584
Microsoft-- Microsoft 365 Copilot	Missing authentication for critical function in M365 Copilot allows an unauthorized attacker to disclose information over a network.	2026-06-18	9.8	CVE-2026-54130
Microsoft-- Microsoft 365 Copilot	Url redirection to untrusted site ('open redirect') in Microsoft 365 Copilot's Business Chat allows an unauthorized attacker to elevate privileges over a network.	2026-06-19	8.8	CVE-2026-47645
Microsoft-- Microsoft Cost Management	Exposure of sensitive information to an unauthorized actor in Cost Management Interactive Experiences allows an unauthorized attacker to disclose information over a network.	2026-06-18	7.5	CVE-2026-47633
Microsoft-- Microsoft Dynamics 365	Improper access control in Microsoft Dynamics 365 allows an authorized attacker to elevate privileges over a network.	2026-06-18	9.9	CVE-2026-47647

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Microsoft Edge (Chromium-based)	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Edge (Chromium-based) allows an authorized attacker to perform spoofing over a network.	2026-06-19	8.8	CVE-2026-32208
Microsoft--Microsoft Exchange Online	Missing authorization in Microsoft Exchange Online allows an authorized attacker to elevate privileges over a network.	2026-06-19	9.6	CVE-2026-48582
Microsoft--Microsoft Malware Protection Engine	Microsoft is aware of an elevation of privilege in the Microsoft Malware Protection Engine in Microsoft Defender publicly referred to as "RoguePlanet". We are working to provide a high quality security update that addresses this vulnerability. We will provide information in this CVE when the update is available.	2026-06-16	7.8	CVE-2026-50656
Microweber--Microweber	A weakness has been identified in Microweber up to 2.0.20. This affects the function userfiles_path of the file /api_nosession/thumbnail_img of the component API Endpoint. Executing a manipulation of the argument cache_path_relative can lead to path traversal. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	7.3	CVE-2026-12198
Mikado-Themes--Ashtanga	Unauthenticated PHP Object Injection in Ashtanga <= 1.2 versions.	2026-06-16	8.1	CVE-2026-40751
Mikado-Themes--ChapterOne	Unauthenticated Local File Inclusion in ChapterOne <= 1.7 versions.	2026-06-17	8.1	CVE-2026-40731
Mikado-Themes--Chateau	Unauthenticated PHP Object Injection in ChÃteau <= 1.2.1 versions.	2026-06-17	8.1	CVE-2026-40757
Mikado-Themes--EasyMeals	Unauthenticated PHP Object Injection in EasyMeals <= 1.5.1 versions.	2026-06-17	8.1	CVE-2026-40753
Mikado-Themes--Esme	Unauthenticated PHP Object Injection in EsmÃe <= 1.4 versions.	2026-06-16	8.1	CVE-2026-40759
Mikado-Themes--Kastell	Unauthenticated Local File Inclusion in Kastell <= 2.0 versions.	2026-06-17	8.1	CVE-2026-52707
Mikado-Themes--LuxeDrive	Unauthenticated PHP Object Injection in LuxeDrive <= 1.4 versions.	2026-06-16	8.1	CVE-2026-40739
Mikado-Themes--Mikado Core	Unauthenticated Local File Inclusion in Mikado Core <= 1.6 versions.	2026-06-17	8.1	CVE-2026-39537
Mikado-Themes--ShiftUp	Unauthenticated PHP Object Injection in ShiftUp <= 1.3 versions.	2026-06-17	8.1	CVE-2026-40733
Mikado-Themes--TechLink	Unauthenticated PHP Object Injection in TechLink <= 1.3 versions.	2026-06-16	8.1	CVE-2026-40755
Mikado-Themes--Zoya	Unauthenticated PHP Object Injection in Zoya <= 1.4 versions.	2026-06-17	8.1	CVE-2026-40756
Monetizemore--Advanced Ads	Improper Control of Generation of Code ('Code Injection') vulnerability in Monetizemore Advanced Ads allows Remote Code Inclusion. This issue affects Advanced Ads: from n/a through 2.0.21.	2026-06-17	7.5	CVE-2026-54816
Montodel--House-Rental-Management	A vulnerability was detected in Montodel House-Rental-Management up to 90010017b81265eb1ef3810268909f7719a33863. Affected by this issue is some unknown functionality of the file /login.php. The manipulation of the argument Username results in sql injection. The attack can be executed remotely. The exploit is now public and may be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	7.3	CVE-2026-12775
Montonio--Montonio for WooCommerce	Unauthenticated Broken Access Control in Montonio for WooCommerce <= 10.1.2 versions.	2026-06-15	7.5	CVE-2026-48873
Motive Commerce	Unauthenticated Broken Access Control in AI Product Search for WooCommerce – Motive Commerce Search <= 1.38.2 versions.	2026-06-15	8.2	CVE-2026-42664

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Search--AI Product Search for WooCommerce Motive Commerce Search				
mra13 / Team Tips and Tricks HQ--Simple Shopping Cart	Unauthenticated Insecure Direct Object References (IDOR) in Simple Shopping Cart <= 5.2.9 versions.	2026-06-15	7.5	CVE-2026-48868
multer--multer	Impact: multer versions 1.0.0 through 2.1.1 and 3.0.0-alpha.1 are vulnerable to a Denial of Service via deeply nested field names in multipart form data. The append-field dependency parses bracket notation in field names with no limit on nesting depth, allowing an attacker to force allocation of deeply nested object structures that consume CPU and memory. A single HTTP request with a crafted multipart body is sufficient to exploit this. Patches: Users should upgrade to multer 2.2.0 (2.x line) or 3.0.0-alpha.2 (3.x prerelease) and configure the new limits.fieldNestingDepth option to the minimum depth their application requires. Workarounds: Set limits.fields to a reasonable value to reduce the number of fields an attacker can send per request. This does not fully mitigate the issue but limits the impact.	2026-06-15	7.5	CVE-2026-5079
Myportfolio--Myportfolio	Joomla Component Myportfolio 3.0.2 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the pid parameter. Attackers can send GET requests to index.php with malicious pid values in the task=project&view=grid endpoint to extract sensitive database information.	2026-06-19	8.2	CVE-2017-20280
Mythemes--my flatonica	Unauthenticated Cross Site Scripting (XSS) in my flatonica <= 0.0.8 versions.	2026-06-17	7.1	CVE-2024-49269
Naked Cat Plugins (by Webdados)--Feed KuntoKusta for WooCommerce Free	Unauthenticated SQL Injection in Feed KuntoKusta for WooCommerce - Free <= 5.3 versions.	2026-06-15	9.3	CVE-2026-39441
NCEAS--metacat	Metacat is data repository software that helps researchers preserve, share, and discover data. Versions 2.0.0 and and above contain an unauthenticated SQL injection in the /harvesterRegistration endpoint. HarvesterRegistration.dbInsert() builds an INSERT against HARVEST_SITE_SCHEDULE via string concatenation, using a quoteString() helper that performs raw single-quote wrapping without escaping. Three request parameters reach the sink: unit, contactEmail, and documentListURL. The servlet does not verify a real LDAP identity. Allowing the vulnerable insert to proceed. Since the PostgreSQL backend permits stacked queries via Statement.executeUpdate(), this vulnerability allows full read/write/execute access in the Metacat database context. The vulnerability was remediated in Metacat 3.0.0.	2026-06-15	9.8	CVE-2026-48114
nesquena--hermes-webui	Hermes WebUI before 0.51.368 contains an authorization bypass vulnerability in the get_profile_cookie() function that accepts unauthenticated profile names from the hermes_profile cookie. An authenticated attacker can forge the hermes_profile cookie value to bypass profile-scoped authorization checks and access sessions, files, and resources across different profiles.	2026-06-17	8.1	CVE-2026-53871
Netdrive--NetDrive	NetDrive 2.6.12 contains an unquoted service path vulnerability in the Netdrive2_Service_Netdrive2 service that allows local users to execute arbitrary code with SYSTEM privileges. Attackers can insert malicious	2026-06-19	7.8	CVE-2016-20092

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	executables in the system root path that will be executed during service startup or system reboot, resulting in privilege escalation.			
Network-Inventory-Advisor--Network Inventory Advisor	Network Inventory Advisor 5.0.26.0 installs the niaservice service with an unquoted binary path that allows local attackers to escalate privileges by placing malicious executables in intermediate directories. Attackers can exploit the unquoted path in the service configuration to execute arbitrary code with LocalSystem privileges when the service starts or restarts.	2026-06-19	7.8	CVE-2019-25747
Networkdls--Fortitude HTTP	Fortitude HTTP 1.0.4.0 contains an unquoted service path vulnerability that allows local users to execute arbitrary code with elevated privileges by exploiting the service binary path. Attackers can insert malicious executables in the system root path that execute with SYSTEM privileges during service startup or system reboot.	2026-06-19	7.8	CVE-2016-20087
Nexi Payments--Nexi XPay	Missing Authorization vulnerability in Nexi Payments Nexi XPay allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Nexi XPay: from n/a through 8.3.1.	2026-06-17	7.5	CVE-2026-54810
nextgeneditor--NextGen Editor	Joomla NextGen Editor 2.1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL commands through the pname parameter. Attackers can send GET requests to index.php with option=com_nge&view=config and inject malicious SQL code in the pname parameter to extract sensitive database information.	2026-06-19	8.2	CVE-2017-20252
NI--grpc-device	There is an untrusted pointer dereference vulnerability in the NI grpc-device sideband streaming API that may allow an attacker to cause an arbitrary memory dereference, potentially resulting in remote code execution. Successful exploitation requires an attacker to supply a specially crafted Moniker protobuf message. This affects NI grpc-device 2.17.0 and prior versions.	2026-06-19	9.1	CVE-2026-48137
NI--grpc-device	There is an insecure default credentials vulnerability in NI grpc-device when TLS configuration is not present and the server is bound beyond loopback. This may allow an unauthenticated user access to the server on the local network. This affects NI grpc-device 2.17.0 and prior versions.	2026-06-19	9.1	CVE-2026-9142
NI--grpc-device	There is an out-of-bounds read vulnerability in the NI grpc-device streaming API due to a missing bounds check that may result in a denial of service. Successful exploitation requires an attacker to supply a specially crafted write request. This affects NI grpc-device 2.17.0 and prior versions.	2026-06-19	7.5	CVE-2026-48138
NI--grpc-device	There is a NULL pointer dereference vulnerability in NI grpc-device in the data moniker service that may allow an attacker to cause a denial of service by triggering a crash. Successful exploitation requires an attacker to provide an unknown value to the data moniker service. This affects NI grpc-device 2.17.0 and prior versions.	2026-06-19	7.5	CVE-2026-48139
Ninja Team--FastDup	Unauthenticated Path Traversal in FastDup <= 2.7.2 versions.	2026-06-15	9.6	CVE-2026-52703
Nordmograph--StreetGuessr Game	Joomla StreetGuessr Game 1.1.8 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the catid parameter. Attackers can send GET requests to index.php with the option=com_streetguess&view=maps parameters and inject SQL code in the catid parameter to extract sensitive database information including version and database names.	2026-06-19	8.2	CVE-2017-20271
NousResearch--hermes-agent	Hermes Agent before 0.16.0 contains a DNS rebinding vulnerability in WebSocket endpoints that allows remote attackers to bypass Host and Origin validation. FastAPI HTTP middleware does not execute for WebSocket upgrade requests on /api/pty, /api/ws, /api/pub, and /api/events endpoints, enabling attackers to exploit DNS rebinding and inject malicious commands or read terminal output.	2026-06-17	7.5	CVE-2026-53869
NSquared--Simply Schedule Appointments	Unauthenticated SQL Injection in Simply Schedule Appointments <= 1.6.9.27 versions.	2026-06-15	9.3	CVE-2026-39493

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
NSquared-- Simply Schedule Appointments	Unauthenticated Cross Site Scripting (XSS) in Simply Schedule Appointments <= 1.6.10.6 versions.	2026-06-15	7.1	CVE-2026-39447
NSquared-- Simply Schedule Appointments	Unauthenticated Sensitive Data Exposure in Simply Schedule Appointments < 1.6.11.2 versions.	2026-06-15	7.5	CVE-2026-42384
Nur-Alam39-- bus-ticket	Nur-Alam39 bus-ticket (no released versions; latest commit 459cabdb99c00225b26e46e3c2c30ae1de7bad) contains an unauthenticated SQL injection vulnerability in bus_info.php. The busid parameter received via HTTP POST is concatenated directly into a MySQL query (select * from bus_info where id=\$busid) without sanitization, escaping, or parameterization, and in a numeric (unquoted) context. A remote, unauthenticated attacker can inject arbitrary SQL - for example a UNION-based payload such as busid=-1 UNION SELECT 1,2,3,4,5,6 - to read arbitrary data from the bus_service database. The application connects to the database as the MySQL root account with an empty password, increasing the potential impact. The query is executed via mysqli_query(), which does not permit stacked (semicolon-separated) statements.	2026-06-18	9.8	CVE-2026-55740
nv-tlabs--GEN3C	NVIDIA Spatial Intelligence Lab's (SIL) GEN3C contains an unauthenticated remote code execution vulnerability in the inference API server where the /request-inference and /seed-model endpoints deserialize raw HTTP request bodies using Python's pickle.loads() without authentication or input validation. Attackers can supply a crafted payload containing a __reduce__ gadget to the inference API port to achieve remote code execution as the inference process.	2026-06-17	9.8	CVE-2026-53805
NVIDIA--NeMo Framework	NVIDIA NeMo Framework for all platforms contains a code injection vulnerability. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, information disclosure, and data tampering.	2026-06-16	7.8	CVE-2026-24155
NVIDIA--NeMo Framework	NVIDIA NeMo Framework for Linux contains a vulnerability where an attacker may cause deserialization of untrusted data. A successful exploit of this vulnerability may lead to code execution, escalation of privileges, data tampering, and information disclosure.	2026-06-16	7.8	CVE-2026-24228
oleksandr-- E2Pdf Export Pdf Tool for WordPress	The E2Pdf - Export Pdf Tool for WordPress plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 1.32.26. This is due to the screen_action() function lacking a dedicated capability check and nonce verification - when invoked via the ?action=screen routing path the controller's index_action() nonce gate is bypassed entirely - while reading an attacker-controlled option name and value from \$_POST['wp_screen_options'] and passing them directly to update_option() with no allowlist, relying solely on the page-level e2pdf_templates capability which the plugin's own Permissions UI allows administrators to grant to any role including Subscriber, Contributor, Author, or Editor. This makes it possible for authenticated attackers, with a custom role that has been granted the e2pdf_templates capability, to overwrite arbitrary WordPress options such as default_role and thereby escalate their privileges to administrator.	2026-06-18	8.8	CVE-2026-12407
OliveTin-- OliveTin	OliveTin gives access to predefined shell commands from a web interface. In versions 3000.0.0 and prior, the template engine uses a single shared text/template.Template instance (tpl package-level variable in service/internal/tpl/templates.go) across all goroutines. Every action execution calls tpl.Parse(source) followed by t.Execute() on this shared instance with no synchronization. When two or more actions execute concurrently (which is the normal case - each ExecRequest spawns a goroutine), a race condition occurs: one goroutine's Parse overwrites the template tree while another goroutine is calling Execute, causing cross-user command contamination, Go runtime panic, and incorrect command execution. This issue has been resolved in version 3000.13.0.	2026-06-15	7.5	CVE-2026-48708

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Omnisend--Email Marketing for WooCommerce by Omnisend	Unauthenticated Broken Authentication in Email Marketing for WooCommerce by Omnisend <= 1.18.0 versions.	2026-06-15	7.5	CVE-2026-42668
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, the terminal-server reverse proxy in `backend/open_webui/routers/terminals.py` does not fully confine the user-controlled `path` segment before forwarding it to an admin-configured terminal server. An authenticated user who has been granted access to a terminal server can craft `path` values containing encoded `../` traversal sequences that escape the intended path (or policy) scope on that server, reaching unintended endpoints and files on the terminal-server host. Where the terminal server fans requests out to internal services, this also gives SSRF-style reach into those services. This is a separate code path from the `/api/v1/retrieval/process/web` SSRF (GHSA-c6xv-rcvw-v685), with its own input. Two distinct vectors are consolidated here: first, raw path forwarding / single-encoded traversal (original report); and second, a bypass of the subsequently-added `_sanitize_proxy_path` mitigation using double-encoded dots (`%252e%252e`). The attacker-controlled input is the request `path`, supplied by the non-admin user, not anything an administrator configures, so this is not an admin-trust / Rule-9 situation. Version 0.9.6 fixes the issue.	2026-06-18	7.7	CVE-2026-54017
OpenClaw--OpenClaw	OpenClaw before 2026.5.26 contains an authorization bypass vulnerability where a surviving pairing-scoped device session can re-establish node token authority after revocation. Attackers with a paired device can regain WebSocket node-level access without renewed approval, weakening revocation controls and maintaining unauthorized access longer than intended.	2026-06-16	8.8	CVE-2026-53843
OpenClaw--OpenClaw	OpenClaw before 2026.5.7 contains a privilege escalation vulnerability where the allowFrom feature improperly validates Discord account identity using mutable display names instead of immutable user IDs. Attackers with Discord accounts can change their display name to match a policy entry and gain unauthorized agent access intended for another Discord identity.	2026-06-16	8.1	CVE-2026-53849
OpenClaw--OpenClaw	OpenClaw before 2026.5.12 contains an argument pattern validation bypass in the exec allowlist that allows attackers to execute disallowed arguments for allowlisted executables on Linux and macOS systems. Attackers can bypass configured argPattern restrictions by directly invoking allowlisted executables with unrestricted arguments, potentially enabling unauthorized file access, network access, or command execution.	2026-06-16	8.3	CVE-2026-53853
OpenClaw--OpenClaw	OpenClaw before 2026.4.2 contains an inline-eval bypass vulnerability allowing authenticated operators to weaken strict allowlist checks via shell positional parameters. Attackers can combine allowlisted tools with shell positional arguments to place inline-eval content in shell carriers outside intended allowlist rules, enabling execution of unapproved shell-provided content.	2026-06-16	8.1	CVE-2026-53855
OpenClaw--OpenClaw	OpenClaw before 2026.5.3 contains a policy enforcement vulnerability where Zalo contacts with mutable display metadata could match allowFrom policy entries through display name changes. Attackers with mutable display names could receive agent responses intended for different Zalo identities when the feature is enabled.	2026-06-16	8.1	CVE-2026-53857
OpenClaw--OpenClaw	OpenClaw before 2026.5.26 contains an insufficient sanitization vulnerability in the host environment sanitizer that allows Node.js control variables to bypass validation. Attackers with access to workspace .env files, tool environment overrides, or skill environment blocks can pass malicious Node.js control variables to influence child processes or coverage output paths.	2026-06-16	8.1	CVE-2026-53864

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
OpenClaw-- OpenClaw	OpenClaw before 2026.5.12 contains an allowlist bypass vulnerability in shell inline-command parsing that allows authenticated operators to execute unapproved commands. A command request using shell inline-command forms could route through a parser case missing the expected allowlist decision, enabling shell content execution without intended approval prompts.	2026-06-16	8.1	CVE-2026-53866
OpenClaw-- OpenClaw	OpenClaw before 2026.5.12 contains an information disclosure vulnerability in streamable-http MCP servers that forwards operator-configured custom headers during cross-origin redirects. Attackers controlling or compromising an MCP endpoint can redirect requests to exfiltrate sensitive headers like API keys or tenant-routing credentials to attacker-controlled origins.	2026-06-16	7.1	CVE-2026-53840
OpenClaw-- OpenClaw	OpenClaw before 2026.5.2 contains an environment variable injection vulnerability allowing workspace .env files to influence Python runtime selection through CLOUDSDK_PYTHON during Gmail setup gcloud execution. Attackers with repository access can manipulate the CLOUDSDK_PYTHON variable to execute setup through unintended local Python paths, potentially enabling arbitrary code execution.	2026-06-16	7.1	CVE-2026-53842
OpenClaw-- OpenClaw	OpenClaw before 2026.4.29 contains a path traversal vulnerability in the install helper that allows workspace .env files to override the npm_execpath configuration used for bundled runtime dependency installation. Attackers with workspace access can execute unintended local package-manager executables during dependency setup to compromise the build environment.	2026-06-16	7.1	CVE-2026-53846
OpenClaw-- OpenClaw	OpenClaw before 2026.5.2 contains an environment variable injection vulnerability where workspace .env STATE_DIRECTORY could influence bundled runtime dependency roots. Attackers can manipulate the STATE_DIRECTORY variable to load runtime dependencies from unintended local paths, potentially executing malicious code during dependency resolution.	2026-06-16	7.1	CVE-2026-53858
OpenClaw-- OpenClaw	OpenClaw before 2026.4.25 contains an input validation vulnerability in tool group policy callers that accept unvalidated group IDs. Attackers who can supply a group ID to the policy resolver could trigger incorrect group-policy decisions for tool invocations, potentially bypassing intended access controls.	2026-06-16	7.1	CVE-2026-53863
OpenClaw-- OpenClaw	OpenClaw before 2026.5.2 contains a path traversal vulnerability in maintenance task execution that allows workspace-derived service paths to influence trash command selection. Attackers can execute unintended local executables from operator-unintended paths during maintenance operations by manipulating workspace-derived environment paths.	2026-06-16	7.1	CVE-2026-53865
Oracle Corporation-- APM - Application Performance Management	Vulnerability in the APM - Application Performance Management product of Oracle Enterprise Manager (component: JADM, JVM Diagnostics). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise APM - Application Performance Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all APM - Application Performance Management accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of APM - Application Performance Management. CVSS 3.1 Base Score 9.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H).	2026-06-16	9.1	CVE-2026-46858
Oracle Corporation-- Identity Manager	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOP to compromise Identity Manager. While the vulnerability is in Identity Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Identity Manager. CVSS 3.1 Base	2026-06-16	9.9	CVE-2026-35268

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).			
Oracle Corporation-- Identity Manager	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: OIM Legacy UI). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Identity Manager. Successful attacks of this vulnerability can result in takeover of Identity Manager. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46807
Oracle Corporation-- Identity Manager	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: Security). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Identity Manager. Successful attacks of this vulnerability can result in takeover of Identity Manager. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-35265
Oracle Corporation-- Identity Manager	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: REST WebServices). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Identity Manager. Successful attacks of this vulnerability can result in takeover of Identity Manager. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-35267
Oracle Corporation-- Identity Manager	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: REST WebServices). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Identity Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Identity Manager accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	2026-06-16	7.5	CVE-2026-35269
Oracle Corporation-- Identity Manager Connector	Vulnerability in the Identity Manager Connector product of Oracle Fusion Middleware (component: Mainframe Connectors). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Identity Manager Connector. While the vulnerability is in Identity Manager Connector, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Identity Manager Connector. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-35294
Oracle Corporation-- Identity Manager Connector	Vulnerability in the Identity Manager Connector product of Oracle Fusion Middleware (component: Generic Unix Connector). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Identity Manager Connector. While the vulnerability is in Identity Manager Connector, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Identity Manager Connector. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46792
Oracle Corporation-- Identity Manager Connector	Vulnerability in the Identity Manager Connector product of Oracle Fusion Middleware (component: Database User). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Identity Manager Connector. While the vulnerability is in	2026-06-16	9.9	CVE-2026-46793

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Identity Manager Connector, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Identity Manager Connector. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).			
Oracle Corporation--Identity Manager Connector	Vulnerability in the Identity Manager Connector product of Oracle Fusion Middleware (component: Generic Unix Connector). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via SSH to compromise Identity Manager Connector. While the vulnerability is in Identity Manager Connector, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Identity Manager Connector. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46794
Oracle Corporation--JD Edwards EnterpriseOne Accounts Payable	Vulnerability in the JD Edwards EnterpriseOne Accounts Payable product of Oracle JD Edwards (component: Accounts Payable). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Accounts Payable. While the vulnerability is in JD Edwards EnterpriseOne Accounts Payable, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Accounts Payable. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46908
Oracle Corporation--JD Edwards EnterpriseOne Accounts Payable	Vulnerability in the JD Edwards EnterpriseOne Accounts Payable product of Oracle JD Edwards (component: Accounts Payable). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Accounts Payable. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all JD Edwards EnterpriseOne Accounts Payable accessible data as well as unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Accounts Payable accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-06-16	8.1	CVE-2026-46891
Oracle Corporation--JD Edwards EnterpriseOne General Ledger	Vulnerability in the JD Edwards EnterpriseOne General Ledger product of Oracle JD Edwards (component: E1 Foundation). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via SMB to compromise JD Edwards EnterpriseOne General Ledger. While the vulnerability is in JD Edwards EnterpriseOne General Ledger, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne General Ledger. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46893
Oracle Corporation--JD Edwards EnterpriseOne Human Resources Management	Vulnerability in the JD Edwards EnterpriseOne Human Resources Management product of Oracle JD Edwards (component: Human Resources). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Human Resources Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all JD Edwards EnterpriseOne Human Resources Management accessible data as well as unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Human Resources Management accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-06-16	9.1	CVE-2026-46892

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation--JD Edwards EnterpriseOne Order Promising	Vulnerability in the JD Edwards EnterpriseOne Order Promising product of Oracle JD Edwards (component: Order Promising Integration). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Order Promising. While the vulnerability is in JD Edwards EnterpriseOne Order Promising, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Order Promising. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46907
Oracle Corporation--JD Edwards EnterpriseOne Project Costing	Vulnerability in the JD Edwards EnterpriseOne Project Costing product of Oracle JD Edwards (component: Job Costing). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Project Costing. While the vulnerability is in JD Edwards EnterpriseOne Project Costing, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all JD Edwards EnterpriseOne Project Costing accessible data as well as unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Project Costing accessible data. CVSS 3.1 Base Score 9.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-06-16	9.6	CVE-2026-46911
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46878
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46879
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46880
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46881

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46882
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46883
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via JDENET to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46904
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46905
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. While the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all JD Edwards EnterpriseOne Tools accessible data as well as unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 9.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-06-16	9.6	CVE-2026-46906
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46909

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Enterprise Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Tools accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H).	2026-06-16	9.1	CVE-2026-46910
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Web Runtime Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. While the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all JD Edwards EnterpriseOne Tools accessible data as well as unauthorized update, insert or delete access to some of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	2026-06-16	9.3	CVE-2026-46912
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Installation Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where JD Edwards EnterpriseOne Tools executes to compromise JD Edwards EnterpriseOne Tools. While the vulnerability is in JD Edwards EnterpriseOne Tools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 9.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.3	CVE-2026-46913
Oracle Corporation--JD Edwards EnterpriseOne Tools	Vulnerability in the JD Edwards EnterpriseOne Tools product of Oracle JD Edwards (component: Business Logic Infrastructure Security). Supported versions that are affected are 9.2.0.0-9.2.26.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in takeover of JD Edwards EnterpriseOne Tools. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46903
Oracle Corporation--MySQL NDB Cluster	Vulnerability in the MySQL NDB Cluster product of Oracle MySQL (component: Cluster: NDB Operator). Supported versions that are affected are 8.0.11-8.0.46, 8.4.0-8.4.9 and 9.0.0-9.7.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise MySQL NDB Cluster. While the vulnerability is in MySQL NDB Cluster, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL NDB Cluster accessible data as well as unauthorized access to critical data or complete access to all MySQL NDB Cluster accessible data. CVSS 3.1 Base Score 9.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-06-16	9.6	CVE-2026-46861
Oracle Corporation--MySQL Router	Vulnerability in the MySQL Router product of Oracle MySQL (component: Router: General). Supported versions that are affected are 9.0.0-9.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise MySQL Router. Successful attacks of this vulnerability can result in takeover of MySQL Router. CVSS 3.1 Base	2026-06-16	9.8	CVE-2026-46860

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation--MySQL Router	Vulnerability in the MySQL Router product of Oracle MySQL (component: Router: General). Supported versions that are affected are 8.4.0-8.4.9 and 9.0.0-9.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise MySQL Router. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Router. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-06-16	7.5	CVE-2026-46862
Oracle Corporation--MySQL Server	Vulnerability in the MySQL Server, MySQL Cluster product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are MySQL Server: 8.4.0-8.4.9, 9.0.0-9.7.0; MySQL Cluster: 8.0.11-8.0.46, 8.4.0-8.4.9 and 9.0.0-9.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server, MySQL Cluster. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server, MySQL Cluster. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2026-06-16	7.5	CVE-2026-46863
Oracle Corporation--MySQL Shell	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell for VS Code). The supported version that is affected is 2026.2.0+9.6.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise MySQL Shell. While the vulnerability is in MySQL Shell, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of MySQL Shell. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46850
Oracle Corporation--MySQL Shell	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell for VS Code). The supported version that is affected is 2026.2.0+9.6.1. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Shell. While the vulnerability is in MySQL Shell, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of MySQL Shell. CVSS 3.1 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	8.5	CVE-2026-46870
Oracle Corporation--Oracle Access Manager	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Access Manager. While the vulnerability is in Oracle Access Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Access Manager. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-35313
Oracle Corporation--Oracle Access Manager	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Web Server Plugin). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Access Manager accessible data as well as unauthorized read access to a subset of Oracle Access Manager accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Access Manager. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity	2026-06-16	7.3	CVE-2026-35314

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).			
Oracle Corporation-- Oracle Advanced Outbound Telephony	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Outbound Telephony accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-06-16	9.1	CVE-2026-46949
Oracle Corporation-- Oracle Advanced Outbound Telephony	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks of this vulnerability can result in takeover of Oracle Advanced Outbound Telephony. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46947
Oracle Corporation-- Oracle Advanced Outbound Telephony	Vulnerability in the Oracle Advanced Outbound Telephony product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks of this vulnerability can result in takeover of Oracle Advanced Outbound Telephony. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46950
Oracle Corporation-- Oracle Agile PLM	Vulnerability in the Oracle Agile PLM product of Oracle Supply Chain (component: Security). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM. Successful attacks of this vulnerability can result in takeover of Oracle Agile PLM. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46859
Oracle Corporation-- Oracle Application Development Framework (ADF)	Vulnerability in the Oracle Application Development Framework (ADF) product of Oracle Fusion Middleware (component: ADF Shared Components). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Application Development Framework (ADF). Successful attacks of this vulnerability can result in takeover of Oracle Application Development Framework (ADF). CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.2	CVE-2026-46769
Oracle Corporation-- Oracle Applications Manager	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Manager. While the vulnerability is in Oracle Applications Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Applications Manager. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46933
Oracle Corporation--	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are	2026-06-16	10	CVE-2026-35307

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Coherence	12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. While the vulnerability is in Oracle Coherence, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Coherence	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Centralized Third Party Jars). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. While the vulnerability is in Oracle Coherence, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	10	CVE-2026-35308
Oracle Corporation-- Oracle Coherence	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-35304
Oracle Corporation-- Oracle Coherence	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Centralized Third Party Jars). The supported version that is affected is 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. While the vulnerability is in Oracle Coherence, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Coherence accessible data as well as unauthorized update, insert or delete access to some of Oracle Coherence accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	2026-06-16	9.3	CVE-2026-35305
Oracle Corporation-- Oracle Coherence	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Centralized Third Party Jars). The supported version that is affected is 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. While the vulnerability is in Oracle Coherence, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Coherence accessible data as well as unauthorized update, insert or delete access to some of Oracle Coherence accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	2026-06-16	9.3	CVE-2026-35306
Oracle Corporation-- Oracle Coherence	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Centralized Third Party Jars). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-35309
Oracle Corporation--	Vulnerability in the Oracle Coherence product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable	2026-06-16	9.8	CVE-2026-35310

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Coherence	vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Coherence. Successful attacks of this vulnerability can result in takeover of Oracle Coherence. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Complex Maintenance, Repair and Overhaul	Vulnerability in the Oracle Complex Maintenance, Repair and Overhaul product of Oracle E-Business Suite (component: Production). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair and Overhaul. While the vulnerability is in Oracle Complex Maintenance, Repair and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Complex Maintenance, Repair and Overhaul. CVSS 3.1 Base Score 8.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	8.5	CVE-2026-46915
Oracle Corporation-- Oracle Complex Maintenance, Repair and Overhaul	Vulnerability in the Oracle Complex Maintenance, Repair and Overhaul product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair and Overhaul. Successful attacks of this vulnerability can result in takeover of Oracle Complex Maintenance, Repair and Overhaul. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.5	CVE-2026-46934
Oracle Corporation-- Oracle Complex Maintenance, Repair and Overhaul	Vulnerability in the Oracle Complex Maintenance, Repair and Overhaul product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair and Overhaul. Successful attacks of this vulnerability can result in takeover of Oracle Complex Maintenance, Repair and Overhaul. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.5	CVE-2026-46935
Oracle Corporation-- Oracle Configure to Order	Vulnerability in the Oracle Configure to Order product of Oracle E-Business Suite (component: Supply to Order Workbench). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Configure to Order. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Configure to Order accessible data as well as unauthorized access to critical data or complete access to all Oracle Configure to Order accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-06-16	8.1	CVE-2026-46939
Oracle Corporation-- Oracle Cost Management	Vulnerability in the Oracle Cost Management product of Oracle E-Business Suite (component: Cost Planning). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Cost Management. Successful attacks of this vulnerability can result in takeover of Oracle Cost Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46929
Oracle Corporation-- Oracle Cost Management	Vulnerability in the Oracle Cost Management product of Oracle E-Business Suite (component: Cost Planning). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Cost Management. Successful attacks of this vulnerability can result in takeover of Oracle Cost Management. CVSS 3.1 Base Score 8.8 (Confidentiality,	2026-06-16	8.8	CVE-2026-46940

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Cost Management	Vulnerability in the Oracle Cost Management product of Oracle E-Business Suite (component: Cost Planning). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Cost Management. Successful attacks of this vulnerability can result in takeover of Oracle Cost Management. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.2	CVE-2026-46938
Oracle Corporation-- Oracle Data Integrator	Vulnerability in the Oracle Data Integrator product of Oracle Fusion Middleware (component: Market Place). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Data Integrator. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Data Integrator accessible data as well as unauthorized access to critical data or complete access to all Oracle Data Integrator accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Data Integrator. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L).	2026-06-16	8.3	CVE-2026-35262
Oracle Corporation-- Oracle Enterprise Asset Management	Vulnerability in the Oracle Enterprise Asset Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.6-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Asset Management. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Asset Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46931
Oracle Corporation-- Oracle Enterprise Asset Management	Vulnerability in the Oracle Enterprise Asset Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Asset Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Asset Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Asset Management. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L).	2026-06-16	7.1	CVE-2026-46932
Oracle Corporation-- Oracle Enterprise Command Center Framework	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. While the vulnerability is in Oracle Enterprise Command Center Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Command Center Framework. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46895
Oracle Corporation-- Oracle Enterprise Command Center Framework	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. While the vulnerability is in Oracle Enterprise Command Center Framework, attacks may	2026-06-16	9.1	CVE-2026-46896

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Command Center Framework. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Enterprise Command Center Framework	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. While the vulnerability is in Oracle Enterprise Command Center Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Command Center Framework accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Command Center Framework accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Command Center Framework. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L).	2026-06-16	9.9	CVE-2026-46897
Oracle Corporation-- Oracle Enterprise Command Center Framework	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. While the vulnerability is in Oracle Enterprise Command Center Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Command Center Framework accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Command Center Framework accessible data. CVSS 3.1 Base Score 9.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-06-16	9.6	CVE-2026-46899
Oracle Corporation-- Oracle Enterprise Command Center Framework	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Enterprise Command Center Framework. While the vulnerability is in Oracle Enterprise Command Center Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Command Center Framework. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46900
Oracle Corporation-- Oracle Enterprise Command Center Framework	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. While the vulnerability is in Oracle Enterprise Command Center Framework, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Command Center Framework accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Command Center Framework accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Enterprise Command Center	2026-06-16	9.9	CVE-2026-46901

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Framework. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L).			
Oracle Corporation-- Oracle Enterprise Command Center Framework	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Enterprise Command Center Framework. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Command Center Framework. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46902
Oracle Corporation-- Oracle Enterprise Command Center Framework	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Core). Supported versions that are affected are V15 and V16. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Enterprise Command Center Framework. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Command Center Framework accessible data as well as unauthorized access to critical data or complete access to all Oracle Enterprise Command Center Framework accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N).	2026-06-16	8.1	CVE-2026-46898
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Discovery Framework). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46832
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Metadata Plugin). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46852
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Metadata Plugin). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Manager Base Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	2026-06-16	9.6	CVE-2026-46853

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Target Management). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46854
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Metadata Plugin). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46855
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Metadata Plugin). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Manager Base Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	2026-06-16	9.6	CVE-2026-46856
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Oracle Management Service). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46857
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Install). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Enterprise Manager Base Platform accessible data as well as unauthorized read access to a subset of Oracle Enterprise Manager Base Platform accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:H/A:H).	2026-06-16	9	CVE-2026-46872

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Deployment Library). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.1	CVE-2026-46875
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Agent Next Gen). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows low privileged attacker with network access via SSH to compromise Oracle Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46864
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Extensibility Framework). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Enterprise Manager Base Platform executes to compromise Oracle Enterprise Manager Base Platform. While the vulnerability is in Oracle Enterprise Manager Base Platform, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	8.2	CVE-2026-46865
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Agent Next Gen). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Enterprise Manager Base Platform as well as unauthorized update, insert or delete access to some of Oracle Enterprise Manager Base Platform accessible data. CVSS 3.1 Base Score 8.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H).	2026-06-16	8.2	CVE-2026-46866
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Extensibility Framework). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.2	CVE-2026-46867
Oracle Corporation-- Oracle Enterprise Manager Base Platform	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Extensibility Framework). Supported versions that are affected are 13.5 and 24.1. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise Oracle Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity	2026-06-16	7.2	CVE-2026-46868

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Financials for EMEA	Vulnerability in the Oracle Financials for EMEA product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Financials for EMEA. Successful attacks of this vulnerability can result in takeover of Oracle Financials for EMEA. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.2	CVE-2026-46969
Oracle Corporation-- Oracle HR Intelligence	Vulnerability in the Oracle HR Intelligence product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle HR Intelligence. Successful attacks of this vulnerability can result in takeover of Oracle HR Intelligence. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.2	CVE-2026-46922
Oracle Corporation-- Oracle HR Intelligence	Vulnerability in the Oracle HR Intelligence product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle HR Intelligence. Successful attacks of this vulnerability can result in takeover of Oracle HR Intelligence. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.2	CVE-2026-46970
Oracle Corporation-- Oracle HR Intelligence	Vulnerability in the Oracle HR Intelligence product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle HR Intelligence. Successful attacks of this vulnerability can result in takeover of Oracle HR Intelligence. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.5	CVE-2026-46971
Oracle Corporation-- Oracle HRMS (UK)	Vulnerability in the Oracle HRMS (UK) product of Oracle E-Business Suite (component: UK Payroll). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle HRMS (UK). Successful attacks of this vulnerability can result in takeover of Oracle HRMS (UK). CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.2	CVE-2026-46953
Oracle Corporation-- Oracle Human Resources	Vulnerability in the Oracle Human Resources product of Oracle E-Business Suite (component: Person). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Human Resources. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Human Resources. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).	2026-06-16	7.5	CVE-2026-46955
Oracle Corporation-- Oracle In-Memory Cost Management for Discrete Industries	Vulnerability in the Oracle In-Memory Cost Management for Discrete Industries product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.12-12.2.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle In-Memory Cost Management for Discrete Industries. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle In-Memory Cost Management for Discrete Industries accessible data as well as unauthorized access to critical data or	2026-06-16	9.1	CVE-2026-46930

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	complete access to all Oracle In-Memory Cost Management for Discrete Industries accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).			
Oracle Corporation-- Oracle iSetup	Vulnerability in the Oracle iSetup product of Oracle E-Business Suite (component: General Ledger Update Transform, Reports). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iSetup. Successful attacks of this vulnerability can result in takeover of Oracle iSetup. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46937
Oracle Corporation-- Oracle iSupplier Portal	Vulnerability in the Oracle iSupplier Portal product of Oracle E-Business Suite (component: Home Page). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle iSupplier Portal. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle iSupplier Portal. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H).	2026-06-16	8	CVE-2026-46894
Oracle Corporation-- Oracle iSupplier Portal	Vulnerability in the Oracle iSupplier Portal product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks of this vulnerability can result in takeover of Oracle iSupplier Portal. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.5	CVE-2026-46957
Oracle Corporation-- Oracle iSupport	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle iSupport. While the vulnerability is in Oracle iSupport, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle iSupport. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.1	CVE-2026-46944
Oracle Corporation-- Oracle iSupport	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle iSupport. While the vulnerability is in Oracle iSupport, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle iSupport. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.1	CVE-2026-46945
Oracle Corporation-- Oracle iSupport	Vulnerability in the Oracle iSupport product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle iSupport. While the vulnerability is in Oracle iSupport, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle iSupport. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.1	CVE-2026-46946
Oracle Corporation-- Oracle	Vulnerability in the Oracle Outsourced Mfg for Discrete Industries product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable	2026-06-16	8.8	CVE-2026-46972

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Outsourced Mfg for Discrete Industries	vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Outsourced Mfg for Discrete Industries. Successful attacks of this vulnerability can result in takeover of Oracle Outsourced Mfg for Discrete Industries. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Outsourced Mfg for Discrete Industries	Vulnerability in the Oracle Outsourced Mfg for Discrete Industries product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Outsourced Mfg for Discrete Industries. Successful attacks of this vulnerability can result in takeover of Oracle Outsourced Mfg for Discrete Industries. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46973
Oracle Corporation-- Oracle Process Manufacturing Process Planning	Vulnerability in the Oracle Process Manufacturing Process Planning product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Process Manufacturing Process Planning. Successful attacks of this vulnerability can result in takeover of Oracle Process Manufacturing Process Planning. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46942
Oracle Corporation-- Oracle Process Manufacturing Product Development	Vulnerability in the Oracle Process Manufacturing Product Development product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Process Manufacturing Product Development. While the vulnerability is in Oracle Process Manufacturing Product Development, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Process Manufacturing Product Development. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46918
Oracle Corporation-- Oracle Process Manufacturing Product Development	Vulnerability in the Oracle Process Manufacturing Product Development product of Oracle E-Business Suite (component: Quality Management Specs). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Process Manufacturing Product Development. Successful attacks of this vulnerability can result in takeover of Oracle Process Manufacturing Product Development. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46916
Oracle Corporation-- Oracle Project Portfolio Analysis	Vulnerability in the Oracle Project Portfolio Analysis product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Project Portfolio Analysis. Successful attacks of this vulnerability can result in takeover of Oracle Project Portfolio Analysis. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46961
Oracle Corporation-- Oracle Project Portfolio Analysis	Vulnerability in the Oracle Project Portfolio Analysis product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Project Portfolio Analysis. Successful attacks of this vulnerability can result in takeover of Oracle Project Portfolio Analysis. CVSS 3.1 Base Score 8.8	2026-06-16	8.8	CVE-2026-46962

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle Project Portfolio Analysis	Vulnerability in the Oracle Project Portfolio Analysis product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Project Portfolio Analysis. Successful attacks of this vulnerability can result in takeover of Oracle Project Portfolio Analysis. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.2	CVE-2026-46960
Oracle Corporation-- Oracle Property Manager	Vulnerability in the Oracle Property Manager product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Property Manager. Successful attacks of this vulnerability can result in takeover of Oracle Property Manager. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.2	CVE-2026-46956
Oracle Corporation-- Oracle Public Sector Financials (International)	Vulnerability in the Oracle Public Sector Financials (International) product of Oracle E-Business Suite (component: Authorization). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Public Sector Financials (International). Successful attacks of this vulnerability can result in takeover of Oracle Public Sector Financials (International). CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46967
Oracle Corporation-- Oracle Public Sector Payroll	Vulnerability in the Oracle Public Sector Payroll product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Public Sector Payroll. Successful attacks of this vulnerability can result in takeover of Oracle Public Sector Payroll. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.2	CVE-2026-46976
Oracle Corporation-- Oracle Quality	Vulnerability in the Oracle Quality product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Quality. Successful attacks of this vulnerability can result in takeover of Oracle Quality. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46951
Oracle Corporation-- Oracle Quality	Vulnerability in the Oracle Quality product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Quality. Successful attacks of this vulnerability can result in takeover of Oracle Quality. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46952
Oracle Corporation-- Oracle Receivables	Vulnerability in the Oracle Receivables product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SOAP to compromise Oracle Receivables. Successful attacks of this vulnerability can result in takeover of Oracle Receivables. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.1	CVE-2026-46927

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle Solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Remote Administration Daemon). The supported version that is affected is 11.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Solaris accessible data as well as unauthorized access to critical data or complete access to all Oracle Solaris accessible data. CVSS 3.1 Base Score 10.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N).	2026-06-16	10	CVE-2026-46978
Oracle Corporation-- Oracle Solaris	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Filesystem). The supported version that is affected is 11.4. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Solaris accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.1 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H).	2026-06-16	7.1	CVE-2026-46914
Oracle Corporation-- Oracle Spares Management	Vulnerability in the Oracle Spares Management product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle Spares Management. Successful attacks of this vulnerability can result in takeover of Oracle Spares Management. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46928
Oracle Corporation-- Oracle Subledger Accounting	Vulnerability in the Oracle Subledger Accounting product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Subledger Accounting. Successful attacks of this vulnerability can result in takeover of Oracle Subledger Accounting. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.5	CVE-2026-46958
Oracle Corporation-- Oracle Subledger Accounting	Vulnerability in the Oracle Subledger Accounting product of Oracle E-Business Suite (component: Internal Operations). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Subledger Accounting. Successful attacks of this vulnerability can result in takeover of Oracle Subledger Accounting. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.5	CVE-2026-46959
Oracle Corporation-- Oracle Unified Directory	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via LDAP to compromise Oracle Unified Directory. Successful attacks of this vulnerability can result in takeover of Oracle Unified Directory. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46773
Oracle Corporation-- Oracle Unified Directory	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via RMI to compromise Oracle Unified Directory. Successful attacks of this vulnerability can result in takeover of Oracle Unified Directory. CVSS 3.1 Base Score 9.8	2026-06-16	9.8	CVE-2026-46774

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation--Oracle Unified Directory	Vulnerability in the Oracle Unified Directory product of Oracle Fusion Middleware (component: OUD Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via LDAP to compromise Oracle Unified Directory. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Unified Directory accessible data as well as unauthorized read access to a subset of Oracle Unified Directory accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Unified Directory. CVSS 3.1 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L).	2026-06-16	8.6	CVE-2026-46776
Oracle Corporation--Oracle Universal Work Queue	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. While the vulnerability is in Oracle Universal Work Queue, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Universal Work Queue. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46963
Oracle Corporation--Oracle Universal Work Queue	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. While the vulnerability is in Oracle Universal Work Queue, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Universal Work Queue. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46964
Oracle Corporation--Oracle Universal Work Queue	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). Supported versions that are affected are 12.2.3-12.2.15. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks of this vulnerability can result in takeover of Oracle Universal Work Queue. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46965
Oracle Corporation--Oracle Universal Work Queue	Vulnerability in the Oracle Universal Work Queue product of Oracle E-Business Suite (component: Work Provider Site Level Administration). Supported versions that are affected are 12.2.3-12.2.15. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Universal Work Queue. Successful attacks of this vulnerability can result in takeover of Oracle Universal Work Queue. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.5	CVE-2026-46966
Oracle Corporation--Oracle Virtual Directory	Vulnerability in the Oracle Virtual Directory product of Oracle Fusion Middleware (component: Virtual Directory Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via LDAP to compromise Oracle Virtual Directory. Successful attacks of this vulnerability can result in takeover of Oracle Virtual Directory. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-35312

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Shared Folders). The supported version that is affected is 7.2.8. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data as well as unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).	2026-06-16	7.5	CVE-2026-35275
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: VMSVGA device). The supported version that is affected is 7.2.8. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	7.5	CVE-2026-46873
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.8. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	7.5	CVE-2026-46974
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.1	CVE-2026-35270
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-35286
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-35316

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-35319
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9	CVE-2026-35320
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-35321
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. While the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-35323
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46766
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-06-16	9.1	CVE-2026-46777
Oracle Corporation--	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is	2026-06-16	9.3	CVE-2026-46785

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle WebCenter Content	affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N).			
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	2026-06-16	9.6	CVE-2026-46786
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).	2026-06-16	9.6	CVE-2026-46789
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N).	2026-06-16	9.3	CVE-2026-46795
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N).	2026-06-16	9.3	CVE-2026-46805

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation--Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46813
Oracle Corporation--Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-35315
Oracle Corporation--Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-35317
Oracle Corporation--Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-35322
Oracle Corporation--Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-35324
Oracle Corporation--Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-35325
Oracle Corporation--Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content	2026-06-16	8	CVE-2026-46787

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	accessible data. CVSS 3.1 Base Score 8.0 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N).			
Oracle Corporation--Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1 Base Score 8.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H).	2026-06-16	8.4	CVE-2026-46788
Oracle Corporation--Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).	2026-06-16	8.7	CVE-2026-46804
Oracle Corporation--Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2026-06-16	8.2	CVE-2026-46806
Oracle Corporation--Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Content accessible data as well as unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).	2026-06-16	8.7	CVE-2026-46808
Oracle Corporation--Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Content. CVSS 3.1	2026-06-16	7.2	CVE-2026-35326

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle WebCenter Content. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebCenter Content, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data as well as unauthorized update, insert or delete access to some of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	2026-06-16	7.6	CVE-2026-35327
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2026-06-16	7.5	CVE-2026-46791
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via RMI to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	10	CVE-2026-46778
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via RMI to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	10	CVE-2026-46781
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOP to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-35280
Oracle Corporation--	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions	2026-06-16	9.9	CVE-2026-35281

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle WebCenter Enterprise Capture	that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOp to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).			
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOp to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-35282
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOp to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-35283
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOp to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-35284
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3, IIOp to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-35285
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via T3 to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46779

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle WebCenter Enterprise Capture	Vulnerability in the Oracle WebCenter Enterprise Capture product of Oracle Fusion Middleware (component: Client Bundle). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Enterprise Capture. While the vulnerability is in Oracle WebCenter Enterprise Capture, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Enterprise Capture. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46782
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	10	CVE-2026-46803
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	10	CVE-2026-46846
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Composer). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46765
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Composer). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46767
Oracle Corporation-- Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9	2026-06-16	9.9	CVE-2026-46802

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).			
Oracle Corporation--Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46814
Oracle Corporation--Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46838
Oracle Corporation--Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46844
Oracle Corporation--Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46845
Oracle Corporation--Oracle WebCenter Portal	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Runtime Tools). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise Oracle WebCenter Portal. While the vulnerability is in Oracle WebCenter Portal, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Portal. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-46847
Oracle Corporation--Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. While the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 10.0	2026-06-16	10	CVE-2026-46798

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).			
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. While the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	10	CVE-2026-46800
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-35293
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-35296
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46797
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46799
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46801
Oracle Corporation-- Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebCenter Sites accessible data as well	2026-06-16	9.1	CVE-2026-46809

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	as unauthorized access to critical data or complete access to all Oracle WebCenter Sites accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).			
Oracle Corporation--Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-35318
Oracle Corporation--Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H).	2026-06-16	8	CVE-2026-46796
Oracle Corporation--Oracle WebCenter Sites	Vulnerability in the Oracle WebCenter Sites product of Oracle Fusion Middleware (component: WebCenter Sites). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in takeover of Oracle WebCenter Sites. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.5	CVE-2026-35295
Oracle Corporation--PeopleSoft Enterprise CS Campus Community	Vulnerability in the PeopleSoft Enterprise CS Campus Community product of Oracle PeopleSoft (component: Security). The supported version that is affected is 9.2.38. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Campus Community. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise CS Campus Community. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.1	CVE-2026-46851
Oracle Corporation--PeopleSoft Enterprise CS Student Financials	Vulnerability in the PeopleSoft Enterprise CS Student Financials product of Oracle PeopleSoft (component: Other). The supported version that is affected is 9.2.38. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Student Financials. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise CS Student Financials accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise CS Student Financials accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2026-06-16	8.1	CVE-2026-46849
Oracle Corporation--PeopleSoft Enterprise PT PeopleTools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Performance Monitor). Supported versions that are affected are 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-35278
Oracle Corporation--	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Weblogic). Supported versions that are	2026-06-16	8.7	CVE-2026-35271

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
PeopleSoft Enterprise PT PeopleTools	affected are 8.61 and 8.62. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. While the vulnerability is in PeopleSoft Enterprise PT PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N).			
Oracle Corporation--PeopleSoft Enterprise PT PeopleTools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Deployment Package). Supported versions that are affected are 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where PeopleSoft Enterprise PT PeopleTools executes to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base Score 8.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.4	CVE-2026-35272
Oracle Corporation--PeopleSoft Enterprise PT PeopleTools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Deployment Package). Supported versions that are affected are 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized update, insert or delete access to some of PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N).	2026-06-16	8.2	CVE-2026-35274
Oracle Corporation--PeopleSoft Enterprise PT PeopleTools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Application Server). Supported versions that are affected are 8.61 and 8.62. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.1	CVE-2026-35276
Oracle Corporation--PeopleSoft Enterprise PT PeopleTools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Performance Monitor). Supported versions that are affected are 8.61 and 8.62. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.1	CVE-2026-35279
Oracle Corporation--PeopleSoft Enterprise PT PeopleTools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Deployment Package). Supported versions that are affected are 8.61 and 8.62. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where PeopleSoft Enterprise PT PeopleTools executes to compromise PeopleSoft Enterprise PT PeopleTools. While the vulnerability is in PeopleSoft Enterprise PT PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base Score 8.2	2026-06-16	8.2	CVE-2026-35288

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).			
Oracle Corporation-- PeopleSoft Enterprise PT PeopleTools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools product of Oracle PeopleSoft (component: Deployment Package). Supported versions that are affected are 8.61 and 8.62. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PT PeopleTools. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.1	CVE-2026-35289
Oracle Corporation-- Siebel Apps - Marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in takeover of Siebel Apps - Marketing. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46884
Oracle Corporation-- Siebel Apps - Marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in takeover of Siebel Apps - Marketing. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46887
Oracle Corporation-- Siebel Apps - Marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in takeover of Siebel Apps - Marketing. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46889
Oracle Corporation-- Siebel Apps - Marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in takeover of Siebel Apps - Marketing. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46890
Oracle Corporation-- Siebel Apps - Marketing	Vulnerability in the Siebel Apps - Marketing product of Oracle Siebel CRM (component: Marketing). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel Apps - Marketing. Successful attacks of this vulnerability can result in takeover of Siebel Apps - Marketing. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46886
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-46919

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 17.0-26.5. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.1	CVE-2026-46920
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Cloud Applications. Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46921
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 17.0-26.5. Difficult to exploit vulnerability allows unauthenticated attacker with access to the physical communication segment attached to the hardware where the Siebel CRM Cloud Applications executes to compromise Siebel CRM Cloud Applications. While the vulnerability is in Siebel CRM Cloud Applications, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	8.3	CVE-2026-46925
Oracle Corporation-- Siebel CRM Cloud Applications	Vulnerability in the Siebel CRM Cloud Applications product of Oracle Siebel CRM (component: Siebel Cloud Manager). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Siebel CRM Cloud Applications executes to compromise Siebel CRM Cloud Applications. While the vulnerability is in Siebel CRM Cloud Applications, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Siebel CRM Cloud Applications. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46926
Oracle Corporation-- Siebel CRM Deployment	Vulnerability in the Siebel CRM Deployment product of Oracle Siebel CRM (component: Database Upgrade). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Siebel CRM Deployment executes to compromise Siebel CRM Deployment. Successful attacks of this vulnerability can result in takeover of Siebel CRM Deployment. CVSS 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	7.8	CVE-2026-46888
Oracle Corporation-- Siebel CRM Integration	Vulnerability in the Siebel CRM Integration product of Oracle Siebel CRM (component: EAI). Supported versions that are affected are 17.0-26.5. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Siebel CRM Integration. Successful attacks of this vulnerability can result in takeover of Siebel CRM Integration. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46885
Oracle Corporation-- WebCenter Content: Imaging	Vulnerability in the WebCenter Content: Imaging product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise WebCenter Content: Imaging. Successful attacks of this vulnerability can	2026-06-16	9.8	CVE-2026-46783

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	result in takeover of WebCenter Content: Imaging. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation-- WebCenter Content: Imaging	Vulnerability in the WebCenter Content: Imaging product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise WebCenter Content: Imaging. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all WebCenter Content: Imaging accessible data as well as unauthorized access to critical data or complete access to all WebCenter Content: Imaging accessible data. CVSS 3.1 Base Score 9.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N).	2026-06-16	9.1	CVE-2026-46784
Oracle Corporation-- WebCenter Content: Imaging	Vulnerability in the WebCenter Content: Imaging product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise WebCenter Content: Imaging. Successful attacks of this vulnerability can result in takeover of WebCenter Content: Imaging. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-46780
Oracle Corporation-- WebLogic Server	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise WebLogic Server. While the vulnerability is in WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	10	CVE-2026-35292
Oracle Corporation-- WebLogic Server	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise WebLogic Server. While the vulnerability is in WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 10.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	10	CVE-2026-35301
Oracle Corporation-- WebLogic Server	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise WebLogic Server. While the vulnerability is in WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.9	CVE-2026-35263
Oracle Corporation-- WebLogic Server	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise WebLogic Server. While the vulnerability is in WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2026-06-16	9.1	CVE-2026-35298

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- WebLogic Server	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0, 14.1.1.0.0, 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise WebLogic Server. Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	9.8	CVE-2026-35300
Oracle Corporation-- WebLogic Server	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all WebLogic Server accessible data as well as unauthorized access to critical data or complete access to all WebLogic Server accessible data. CVSS 3.1 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).	2026-06-16	8.7	CVE-2026-35258
Oracle Corporation-- WebLogic Server	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-35259
Oracle Corporation-- WebLogic Server	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise WebLogic Server. Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-35299
Oracle Corporation-- WebLogic Server	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).	2026-06-16	8.3	CVE-2026-35302
Oracle Corporation-- WebLogic Server	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise WebLogic Server. Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	8.8	CVE-2026-35303
Oracle Corporation-- WebLogic Server	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise WebLogic Server. Successful attacks of this vulnerability can result in takeover of WebLogic	2026-06-16	8.8	CVE-2026-35311

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Server. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).			
Oracle Corporation--WebLogic Server	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 14.1.2.0.0 and 15.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where WebLogic Server executes to compromise WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in WebLogic Server, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all WebLogic Server accessible data as well as unauthorized access to critical data or complete access to all WebLogic Server accessible data. CVSS 3.1 Base Score 7.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N).	2026-06-16	7.9	CVE-2026-46848
Ovatheme--BookPro	Unauthenticated Arbitrary File Deletion in BookPro <= 1.1.0 versions.	2026-06-17	8.6	CVE-2026-27400
Paolo--GeoDirectory	Unauthenticated SQL Injection in GeoDirectory <= 2.8.152 versions.	2026-06-15	9.3	CVE-2026-39512
park_of_ideas--Moderno	Unauthenticated PHP Object Injection in Moderno < 1.43 versions.	2026-06-17	9.8	CVE-2026-49108
Passionate Programmer Peter--WP Data Access	Unauthenticated SQL Injection in WP Data Access <= 5.5.70 versions.	2026-06-15	9.3	CVE-2026-42665
Paul--iControlWP	Unauthenticated Privilege Escalation in iControlWP <= 5.5.3 versions.	2026-06-15	9.8	CVE-2026-34901
PerryTS--perry	Perry before 0.5.1166 contains a JWT validation vulnerability that allows remote attackers to bypass token expiration by exploiting the unconditional setting of validate_exp = false in the verify_decode helper within the stdlib JWT verification path. Attackers in possession of a previously issued bearer token can present expired tokens to any jwt.verify() call and retain authenticated access indefinitely, bypassing force-expired sessions such as user logout or administrative revocation.	2026-06-16	9.1	CVE-2026-53776
Personifyinc--Chromacam	Chromacam 4.0.3.0 contains an unquoted service path vulnerability in the PsyFrameGrabberService that allows local attackers to execute arbitrary code by placing malicious executables in unquoted path directories. Attackers with write access to C:\ or subdirectories like C:\Program Files (x86)\Personify\ can place a malicious Program.exe or PsyFrameGrabberService.exe file that executes with LocalSystem privileges when the service starts automatically at boot.	2026-06-19	7.8	CVE-2023-54353
pgadmin.org--pgAdmin 4	Read-only transaction bypass in the pgAdmin 4 AI Assistant allows an attacker who can influence database content that the assistant reads to execute arbitrary SQL with the privileges of the pgAdmin user's database role. The AI Assistant's execute_sql_query tool runs LLM-generated SQL inside a BEGIN TRANSACTION READ ONLY wrapper to prevent data modification. The LLM-supplied query was forwarded to the database driver without restriction to a single statement or to read-only verbs, so a multi-statement payload beginning with COMMIT, END, ROLLBACK, or ABORT terminated the read-only transaction and ran subsequent statements in autocommit mode. The trailing ROLLBACK then had no effect. Delivery is via prompt injection: an attacker who can write content into any object the AI Assistant may inspect (a row, a column value, a comment) can cause the LLM to emit the multi-statement payload as a tool call. With ordinary write privileges on the pgAdmin user's role the attacker can perform unauthorised data modification. When the pgAdmin user's role is a PostgreSQL superuser or holds pg_execute_server_program, the chain extends to remote code execution on the database server host via COPY ... TO PROGRAM. Fix validates the	2026-06-18	9	CVE-2026-12045

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	LLM-supplied query up front: it must parse to exactly one non-empty / non-comment statement whose leading real token (after stripping whitespace, comments, and punctuation) is one of SELECT, WITH, EXPLAIN, SHOW, VALUES, or TABLE. Transaction-control verbs, DML, DDL, CALL, COPY, DO, SET/RESET, and everything else are rejected before any database work happens. PostgreSQL's READ ONLY mode continues to backstop data-modifying CTEs, EXPLAIN ANALYZE on writes, and volatile side effects. This issue affects pgAdmin 4: from 9.13 before 9.16.			
pgadmin.org-- pgAdmin 4	Two state-mutating endpoints in pgAdmin 4's SQL Editor blueprint -- DELETE /sqleditor/close/<trans_id> and POST /sqleditor/initialize/sqleditor/update_connection/<sgid>/<sid>/<did> -- were the only routes in the module missing the @pga_login_required decorator. Both reach a pickle.loads sink on session['gridData']['<trans_id>']['command_obj']: the close endpoint via close_sqleditor_session(), and update_sqleditor_connection via check_transaction_status(). In server mode these endpoints were reachable without any authenticated pgAdmin session. The defect is a missing-authentication-on-critical-function (CWE-306) wrapper around a deserialization-of-untrusted-data sink (CWE-502). Exploiting it for remote code execution requires the attacker to also forge a server-side session file whose gridData entry contains a malicious pickle payload, which in turn requires both (a) knowledge of pgAdmin's Flask SECRET_KEY (no chain to leak it is described here -- the attacker must already possess it) and (b) write access to pgAdmin's sessions/ directory on the host. Neither precondition is granted by this defect on its own. When those preconditions are met from another channel (misconfigured deployment, prior compromise, leaked configuration), the missing auth gate is the final hop that turns an existing partial compromise into unauthenticated code execution in the pgAdmin process -- and, by extension, on the host under whatever account runs pgAdmin. Fix is a one-line @pga_login_required decorator on each of the two endpoints, matching the convention used by every other route in the module. The is_authenticated / MFA chain now runs before the trans_id is dereferenced, so an unauthenticated request is rejected before reaching the deserialization path. The defect is server-mode only. In DESKTOP mode pgAdmin's before_request hook re-authenticates DESKTOP_USER on every request, so no endpoint can be exercised in an unauthenticated state and no auth decorator (or its absence) is meaningful. The accompanying regression test mirrors the attacker's path -- harvests an X-pgA-CSRFToken from GET /login and replays it against both endpoints -- and self-skips outside server mode for that reason; it is wired into the existing server-mode CI workflow alongside the data-isolation tests. This issue affects pgAdmin 4: from 6.9 before 9.16.	2026-06-18	9	CVE-2026-12046
pgadmin.org-- pgAdmin 4	Stored cross-site scripting in pgAdmin 4's error-rendering and plan-node-rendering paths. Text returned by a PostgreSQL server (ErrorResponse messages, including object names quoted back inside relation-does-not-exist errors and inside EXPLAIN Recheck Cond / Exact Heap Blocks fields) was passed verbatim through html-react-parser at every user-facing sink - the notifier toasts, FormFooterMessage / FormInput help and error areas, FormNote, ModalProvider AlertContent and confirmDelete, ToolErrorView, the Explain visualiser's NodeText panel, the SQL editor confirm dialogs, ConfirmSaveContent, PreferencesHelper modal alerts, and SelectThemes helper text. A PostgreSQL server an attacker controls - or any server returning attacker-influenced text such as a table or column name a low-privilege database user can create - could inject arbitrary HTML (including <iframe>) into the pgAdmin DOM the moment the victim's pgAdmin connected to that server or viewed an Explain plan that referenced the crafted object. The injected iframe's srcdoc could fetch attacker-served JavaScript and, by writing to parent.location, redirect the victim's top-level pgAdmin browser tab to an attacker-controlled URL.	2026-06-18	9.3	CVE-2026-12048

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Because the injection originates from inside pgAdmin's own interface, standard anti-clickjacking controls (X-Frame-Options, Content-Security-Policy: frame-ancestors) do not mitigate it. A phishing page rendered inside the legitimate pgAdmin window is indistinguishable from a genuine pgAdmin dialog. Fix combines three complementary layers. (1) DOMPurify sanitisation is wrapped around every html-react-parser call site reachable from notifier, alert, form-error, Explain, and SQL-editor flows. (2) A new plain-text rendering contract - SafeMessage / SafeHtmlMessage components plus Notifier.errorText / alertText / warningText / infoText / successText helpers - is introduced; around fifty callers across browser, tools, dashboard, debugger, misc, IIm, preferences, schema diff, and the SQL editor that previously interpolated backend-derived strings are migrated to the plain-text variants. (3) Backend HTML-escape is applied at the post-connection-SQL handler (execute_post_connection_sql) via a new sanitize_external_text helper, so third-party JSON consumers (audit logs, API clients) never receive raw markup either; the Explain plan-info renderer is also patched to .escape Recheck Cond and Exact Heap Blocks at construction (matching every sibling field), giving defence in depth even before DOMPurify runs. This issue affects pgAdmin 4: from 6.0 before 9.16.			
pgadmin.org--pgAdmin 4	SQL injection in pgAdmin 4 across every dialog template that renders ``COMMENT ON ... IS '<description>'' for a user-supplied description field. The Jinja templates for Domains (and their constraints), Foreign Tables, Languages, and Event Triggers, plus the Views OID-lookup query, interpolated the description directly inside a single-quoted SQL literal -- ``{{ data.description }}'' -- instead of passing it through the ``qtLiteral'' escape filter. An authenticated pgAdmin user with permission to create or alter the affected object types could submit a description containing an apostrophe, break out of the literal and chain arbitrary SQL. The injected SQL runs under the PostgreSQL role the user is already authenticated as; for a connected role with ``COPY ... TO/FROM PROGRAM'' (typically PostgreSQL superuser), this chains to OS command execution on the PostgreSQL host. The defect does not cross a privilege boundary -- the user already has direct SQL access to that role through pgAdmin's Query Tool -- so the attacker gains no capability beyond what their database role already grants. The marginal impact captures bypass of any application-layer Query Tool gating an operator may have configured. The defect was originally reported against the Domain Dialog ``description'' field; a code-wide audit identified sixteen sites of the same pattern across the templates listed above. The same review also surfaced ten related sinks in the pgstattuple/pgstatindex stats templates -- ``pgstattuple('{{schema}}.{{table}}')'' and the matching pgstatindex shape - where ``qtIdent'' escapes embedded double quotes inside the identifier but not apostrophes, so a user with CREATE privilege on a schema could plant a table or index named ``foo'bar'' and a later stats viewer would render an unbalanced literal. Fix is layered: 1. Sites: replace every ``{{ x.description }}'' with ``{{ x.description qtLiteral(conn) }}'' (no surrounding quotes -- the filter wraps the value in escaped quotes itself). Plumb ``conn=self.conn'' through every ``render_template'' call that loads one of these templates. Also corrects a ``{ % elif'' Jinja typo in the foreign-table schema diff (dead branch). Rewrite the ten pgstattuple/pgstatindex stats sites to address the relation via OID + ``::oid::regclass'' cast (e.g. ``pgstattuple({{ tid }}::oid::regclass)`'), eliminating the embedded literal-call form entirely so that bug-class can no longer recur there. 2. Driver hardening: ``qtLiteral'' (in ``utils/driver/psycopg3/__init__.py'') used to silently return the raw unescaped value when its ``conn'' argument was falsy. It now raises ``ValueError'' -- surfacing the entire bug class going forward. The change immediately uncovered eight latent plumbing bugs (in ``schemas/__init__.py'', ``schemas/functions/__init__.py'',	2026-06-18	8.8	CVE-2026-12044

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	``schemas/tables/utis.py``, ``foreign_servers/__init__.py``, and seven sites in ``roles/__init__.py``) -- all fixed as part of this patch. The inner ``except`` block that swallowed adapter-level failures and returned the raw value is also removed, so unadaptable inputs raise instead of leaking unescaped values. 3. Regression tests: a per-template behavioural test renders each previously-vulnerable template with an apostrophe-injection payload and asserts the escaped fragment is present and the vulnerable fragment absent; a lint test walks every ``*.sql`` template flagging any ``{{ ... }}`` single-quote-wrapped interpolation against an explicit allowlist; unit tests cover the new qTLiteral fail-fast and inner-except raise paths. This issue affects pgAdmin 4: from 1.0 before 9.16.			
php-standard-library--php-standard-library	PHP Standard Library (PSL) is set of APIs covering async, collections, networking, I/O, cryptography, terminal UI, etc. In versions 6.1.0, 6.1.1 and 6.2.0, the Psl\H2\ServerConnection does not validate that the total bytes received in DATA frames match the content-length header declared in the HEADERS frame, allowing request smuggling. This is in violation of RFC 9113 Â§8.1.1. A malicious client is able to send more DATA bytes than declared, smuggling additional content past application-level size limits and send fewer DATA bytes than declared and close the stream early, causing applications that trust the declared length to behave incorrectly. The vulnerability is only reachable for consumers using Psl\H2\ServerConnection directly to accept untrusted client traffic. Consumers of documented high-level PSL APIs are not affected. This issue has been fixed in versions 6.1.2 and 6.2.1.	2026-06-17	7.5	CVE-2026-48979
phpMyFAQ--phpMyFAQ	phpMyFAQ before 4.1.4 contains missing authorization vulnerabilities in editUser() and updateUserRights() endpoints that allow authenticated administrators to escalate privileges. Non-SuperAdmin users with edit_user permission can set is_superuser flag or grant arbitrary rights to escalate to SuperAdmin access.	2026-06-21	8.8	CVE-2026-56396
PickleScan--PickleScan	PickleScan before 0.0.33 fails to include thepty.spawn function in its unsafe globals list, allowing attackers to bypass security checks. Malicious actors can craft pickle payloads usingpty.spawn to achieve arbitrary code execution when files are processed by PickleScan.	2026-06-17	8.8	CVE-2025-71322
picklescan--picklescan	picklescan before 1.0.4 fails to block pkgutil.resolve_name, allowing attackers to bypass the entire blocklist by resolving any dangerous function through indirect REDUCE calls. Remote attackers can invoke any blocked function such as os.system, builtins.exec, or subprocess.call to achieve remote code execution.	2026-06-17	10	CVE-2026-3490
picklescan--picklescan	picklescan before 0.0.33 contains an incomplete deny-list that fails to blockpydoc.locate and operator.methodcaller functions, allowing attackers to bypass security checks. Remote attackers can craft malicious pickle files using these unblocked functions to achieve arbitrary code execution when the pickle is deserialized.	2026-06-17	9.8	CVE-2025-71320
picklescan--picklescan	picklescan before 0.0.33 contains an arbitrary file writing vulnerability that allows attackers to bypass the dangerous blocklist by using distutils.file_util.write_file. Attackers can construct malicious pickle objects to overwrite critical system files and achieve denial of service or remote code execution.	2026-06-17	9.8	CVE-2025-71321
picklescan--picklescan	picklescan before 0.0.33 fails to block the ctypes module, allowing attackers to achieve remote code execution by invoking direct syscalls and accessing raw memory. Attackers can craft malicious pickle files using ctypes.WinDLL to load kernel32.dll and execute arbitrary commands, bypassing sandbox protections and gadget chain detection.	2026-06-17	9.8	CVE-2025-71323
picklescan--picklescan	picklescan before 0.0.27 contains a parsing logic error in the _list_globals function when handling STACK_GLOBAL opcodes, failing to track arguments in the correct range and allowing malicious pickle files to bypass detection. Attackers can craft pickle files with arguments at position zero to trigger unexpected exceptions and evade security scanning.	2026-06-17	9.8	CVE-2025-71325

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
picklescan--picklescan	picklescan before 1.0.4 contains an incomplete blacklist for the profile module that fails to block the module-level profile.run() function, allowing attackers to achieve arbitrary code execution via exec(). Attackers can craft malicious pickle files calling profile.run(statement) to execute arbitrary Python code while picklescan reports zero security issues.	2026-06-17	9.8	CVE-2026-53873
picklescan--picklescan	picklescan before 1.0.1 contains an unsafe deserialization vulnerability allowing unauthenticated users to execute arbitrary code by hiding eval calls nested under callable objects via getattr. Attackers can embed malicious code in pickle files that evades detection but executes when the pickle is loaded from untrusted sources.	2026-06-17	9.8	CVE-2026-53874
picklescan--picklescan	picklescan before 0.0.28 fails to detect malicious pickle files that invoke torch.utils._config_module.load_config function within reduce methods. Attackers can craft pickle files embedding arbitrary code that evades detection but executes during pickle.load, enabling remote code execution in supply chain attacks.	2026-06-21	8.1	CVE-2025-71348
picklescan--picklescan	picklescan before 0.0.30 fails to detect malicious pickle files using idlelib.pyshell.ModifiedInterpreter.runcommand in reduce methods. Attackers can embed undetected code in pickle files that executes remote commands when loaded by victims.	2026-06-21	8.1	CVE-2025-71357
picklescan--picklescan	picklescan before 0.0.30 fails to detect cProfile.runctx function calls in pickle file reduce methods, allowing attackers to execute arbitrary code. Malicious pickle files bypass picklescan detection and execute remote code when loaded via pickle.load().	2026-06-21	8.1	CVE-2025-71378
picklescan--picklescan	picklescan before 0.0.35 contains an unsafe pickle deserialization vulnerability allowing unauthenticated attackers to read arbitrary server files by chaining io.FileIO and urllib.request.urlopen. Attackers can bypass RCE-focused blocklists to exfiltrate sensitive data like /etc/passwd to external servers.	2026-06-17	7.5	CVE-2026-53872
Pimcore GmbH--Pimcore CMS/DXP	Pimcore CMS/DXP version 12.3.8 contains a sandbox bypass vulnerability that allows authenticated administrative attackers to execute arbitrary methods on PHP objects by exploiting empty checkMethodAllowed() and checkPropertyAllowed() implementations in the custom Twig SecurityPolicy. Attackers can supply malicious Twig templates through the DataObject ClassDefinition Layout\Text component to perform arbitrary file reads, execute arbitrary database queries, and potentially achieve remote code execution via PHP object gadget chains, with the pimcore_* function wildcard further broadening the bypass to all Pimcore Twig functions.	2026-06-17	7.2	CVE-2026-11407
Pods Framework--Pods	Unauthenticated Cross Site Scripting (XSS) in Pods <= 3.3.8 versions.	2026-06-16	7.1	CVE-2026-54191
pontedilana--php-weasyprint	PhpWeasyPrint is a PHP library allowing PDF generation from a URL or an HTML page. Prior to version 2.5.1, `pontedilana/php-weasyprint` builds the shell command for WeasyPrint by passing the binary path through `escapeshellarg()` first and then checking the *quoted* result with `is_executable()`. On POSIX `escapeshellarg('/usr/local/bin/weasyprint')` returns `'/usr/local/bin/weasyprint'` with the single-quote characters as part of the string, so `is_executable()` looks for a file whose actual name includes those quotes. That file never exists, the "safe" branch is dead code, and the raw `\$binary` string (set via the constructor or `setBinary()`) flows directly into `Symfony\Component\Process\Process::fromShellCommandline()`. Any deployment whose binary path is sourced from configuration, an environment variable, or a per-tenant setting reaches a shell-command-injection sink. The library is documented as a one-to-one substitute for KnpLabs/snappy and inherited the exact pre-fix codepath KnpLabs patched in GHSA-vpr4-p6fq-85jc. PhpWeasyPrint version 2.5.1 contains a patch for the issue.	2026-06-19	8.2	CVE-2026-49260

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
pontedilana--php-weasyprint	PhpWeasyPrint is a PHP library allowing PDF generation from a URL or an HTML page. Prior to version 2.6.0, `pontedilana/php-weasyprint` guarded the output filename against the `phar://` stream wrapper with a case-sensitive blacklist. PHP stream wrappers are case-insensitive, so `PHAR://`, `Phar://`, etc. bypass the check and reach `fileExists()` (`file_exists()`) in `prepareOutput()`. On PHP 7 (which the library still supports - PHP 7.4+), this triggers deserialization of a crafted PHAR archive's metadata, leading to remote code execution. This is the patch-bypass of CVE-2023-28115. The same issue and fix were handled upstream in KnpLabs/snappy (GHS-92rv-4j2h-8mjj). PhpWeasyPrint version 2.6.0 contains a patch for the issue.	2026-06-19	8.1	CVE-2026-49286
Powerpackelements--PowerPack Pro for Elementor	Unauthenticated Broken Authentication in PowerPack Pro for Elementor < v2.13.0 versions.	2026-06-17	8.8	CVE-2026-42629
PraisonAI--PraisonAI	PraisonAI before 4.5.128 contains an arbitrary shell command execution vulnerability where the UI modules hardcode approval_mode to auto, overriding administrator configuration from PRAISON_APPROVAL_MODE environment variable. Authenticated attackers can instruct the LLM agent to execute arbitrary shell commands via subprocess.run with shell=True, bypassing the manual approval gate and insufficient command sanitization blocklists.	2026-06-18	8.8	CVE-2026-56075
PraisonAI--PraisonAI	PraisonAI before 1.5.128 contains a cross-origin agent execution vulnerability in the AGUI endpoint that allows remote attackers to trigger arbitrary agent execution. The POST /agui endpoint lacks authentication and hardcodes Access-Control-Allow-Origin: * headers, combined with Starlette's Content-Type-agnostic JSON parsing, enabling attackers to bypass CORS preflight checks via simple requests and exfiltrate sensitive agent responses including tool execution results and environment data.	2026-06-18	8.1	CVE-2026-56076
PraisonAI--PraisonAI	PraisonAI before 1.5.115 contains a path traversal vulnerability in MultiAgentMonitor that fails to sanitize agent IDs when building file paths. Attackers can include traversal sequences like ../ in agent IDs to read, write, or overwrite arbitrary files, enabling sensitive disclosure, denial of service, or code execution.	2026-06-18	8.8	CVE-2026-56078
PremiumPress Limited.--WordPress Dating Theme	Unauthenticated Cross Site Request Forgery (CSRF) in WordPress Dating Theme <= 11.2.0 versions.	2026-06-17	8.8	CVE-2026-22342
PremiumPress Limited.--WordPress Dating Theme	Unauthenticated Broken Access Control in WordPress Dating Theme <= 11.2.0 versions.	2026-06-17	8.6	CVE-2026-22343
premmmerce--Premmerce Dev Tools	The Premmerce Dev Tools plugin for WordPress is vulnerable to Remote Code Execution via missing authorization in versions up to and including 2.0. This is due to the 'generatePluginHandler' function lacking any authorization check before processing user-supplied POST data, combined with the 'createFromStub' function performing unsanitized string substitution of the 'premmmerce_plugin_namespace' parameter directly into PHP stub files written to the wp-content/plugins/ directory. An attacker can inject a semicolon followed by arbitrary PHP code into the namespace parameter, causing the generated plugin file to contain and execute that code when accessed via HTTP. This makes it possible for authenticated attackers with Subscriber-level access and above to create arbitrary PHP files on the server and achieve remote code execution.	2026-06-16	8.8	CVE-2026-6933
PressLayouts--Alukas	Unauthenticated PHP Object Injection in Alukas < 3.0.0 versions.	2026-06-17	8.1	CVE-2026-39445
PressLayouts--EmailShop	Unauthenticated PHP Object Injection in EmailShop <= 2.4.21 versions.	2026-06-16	8.1	CVE-2026-39443

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
PressLayouts--Kapee	Unauthenticated PHP Object Injection in Kapee < 1.7.0 versions.	2026-06-16	8.1	CVE-2026-39446
PressLayouts--Kapee	Unauthenticated Cross Site Scripting (XSS) in Kapee < 1.7.1 versions.	2026-06-17	7.1	CVE-2026-41557
PressLayouts--PressMart	Unauthenticated PHP Object Injection in PressMart <= 1.2.26 versions.	2026-06-17	8.1	CVE-2026-39442
Prince--Integrate Google Drive	Missing Authorization vulnerability in Prince Integrate Google Drive allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Integrate Google Drive: from n/a through 1.3.8.	2026-06-17	8.3	CVE-2024-32949
Projectopia--Projectopia	Custom role Insecure Direct Object References (IDOR) in Projectopia <= 5.1.25.2 versions.	2026-06-15	7.5	CVE-2025-59133
Pulseextensions--Flip Wall	Joomla! Component Flip Wall 8.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the wallid parameter. Attackers can send GET requests to index.php with the option=com_flipwall&task=click&wallid parameter containing SQL injection payloads to extract sensitive database information.	2026-06-19	7.1	CVE-2017-20265
Pulseextensions--Sponsor Wall	Joomla! Component Sponsor Wall 8.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the wallid parameter. Attackers can send GET requests to index.php with the option=com_sponsorwall&task=click&wallid parameter containing SQL injection payloads to extract sensitive database information including credentials and configuration data.	2026-06-19	7.1	CVE-2017-20264
Qihoo--360 Total Security	A security flaw has been discovered in Qihoo 360 Total Security 6.0. This vulnerability affects the function RpcStringBindingComposeW of the component Nucleus Engine Monitoring Logic. Performing a manipulation of the argument NetworkAddr results in protection mechanism failure. The attack requires a local approach. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	7.8	CVE-2026-12214
QuantumCloud--ChatBot	Subscriber Broken Access Control in ChatBot <= 7.9.7 versions.	2026-06-15	7.1	CVE-2026-40788
QuantumCloud--Conversational Forms for ChatBot	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in QuantumCloud Conversational Forms for ChatBot allows Path Traversal. This issue affects Conversational Forms for ChatBot: from n/a through 1.1.8.	2026-06-17	7.5	CVE-2024-32729
QuantumCloud--WPBot Pro Wordpress Chatbot	Subscriber Arbitrary File Deletion in WPBot Pro Wordpress Chatbot <= 13.6.5 versions.	2026-06-17	7.7	CVE-2025-60223
quarkusio--quarkus	Quarkus is a Java framework for building cloud-native applications. Prior to versions 3.37.0, 3.36.3, 3.33.2.1, 3.33.3, 3.27.4.1, 3.27.5, and 3.20.6.2, Quarkus HTTP path-based authorization policies can be bypassed using encoded semicolons (%3B) to smuggle matrix parameters past the security layer, and using encoded slashes (%2F) or backslashes (%5C) to access protected static resources. This is a distinct issue from CVE-2026-39852, which addressed only literal semicolon stripping. Versions 3.37.0, 3.36.3, 3.33.2.1, 3.33.3, 3.27.4.1, 3.27.5, and 3.20.6.2 contain a patch.	2026-06-19	7.5	CVE-2026-50559
Radiflow--iSAP Smart Collector	The device has a webserver that exposes a REST API authenticated with a token on the management network. By exploiting an OS command injection vulnerability an authenticated attacker can send arbitrary commands to the device that are executed with administrative permissions by the underlying operating system.	2026-06-16	9.1	CVE-2026-22313
Radiflow--iSAP Smart Collector	The device has a webserver that exposes a REST API authenticated with a constant token. The unauthenticated API can be used by an attacker to get access to system settings, modify the configuration and execute some commands (e.g. system reboot).	2026-06-16	8.6	CVE-2026-22312

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rainafarai--Notification for Telegram	Unauthenticated Cross Site Scripting (XSS) in Notification for Telegram <= 3.5 versions.	2026-06-15	7.1	CVE-2026-40732
Raindropsinfotec--Twitch Tv	Joomla! Component Twitch Tv 1.1 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the username and id parameters. Attackers can send GET requests to index.php with option=com_twitchtv and view parameters containing SQL injection payloads to extract sensitive database information including credentials and configuration data.	2026-06-19	8.2	CVE-2017-20270
Real--RealTimes Desktop Service	RealTimes Desktop Service 18.1.4 contains an unquoted service path vulnerability in the rpdsvc.exe binary that allows local attackers to escalate privileges. Attackers can place malicious executables in unquoted path directories to execute arbitrary code with LocalSystem privileges during service startup or system reboot.	2026-06-19	7.8	CVE-2020-37251
Really Simple Plugins--Really Simple SSL	Unauthenticated Broken Authentication in Really Simple SSL <= 9.5.10 versions.	2026-06-15	8.1	CVE-2026-48970
RealMag777--InPost Gallery	Unauthenticated SQL Injection in InPost Gallery <= 2.1.4.6 versions.	2026-06-16	9.3	CVE-2026-39574
Realtek--Realtek Audio Service	Realtek Audio Service 1.0.0.55 contains an unquoted service path vulnerability in RtkAudioService64.exe that allows local attackers to escalate privileges by injecting malicious code. Attackers can place executable files in the unquoted service path directory to execute arbitrary code with LocalSystem privileges during service startup or system reboot.	2026-06-19	7.8	CVE-2020-37252
Realtek--Realtek High Definition Audio Driver	Realtek High Definition Audio Driver 6.0.1.6730 contains an unquoted service path vulnerability that allows local attackers to escalate privileges by placing a malicious executable in the service path. Attackers can insert an executable file in the unquoted path and restart the service to execute code with LocalSystem privileges.	2026-06-19	7.8	CVE-2016-20085
Realtyna--Realtyna Organic IDX plugin	Unauthenticated SQL Injection in Realtyna Organic IDX plugin <= 5.1.0 versions.	2026-06-15	9.3	CVE-2026-45439
Red Hat--Red Hat Ansible Automation Platform 2	A command injection vulnerability was found in galaxy_ng. The do_git_checkout() function in the legacy role import API (v1) interpolates unsanitized git ref names (branch/tag names) into shell commands executed via subprocess.run() with shell=True. An authenticated user who controls a git repository can create a branch or tag with shell metacharacters in the name to achieve remote code execution on the pulp worker. The vulnerable endpoint is only reachable when GALAXY_ENABLE_LEGACY_ROLES is set to True, which is not the default configuration.	2026-06-16	7.5	CVE-2026-12398
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in Pacemaker. An unauthenticated remote attacker can exploit an integer overflow vulnerability in the remote message decompression process. By sending a specially crafted compressed remote message before authentication, an attacker can cause memory corruption, leading to a denial of service (DoS) in the CIB remote listener. This can result in the affected service crashing.	2026-06-16	8.6	CVE-2026-10649
Red Hat--Red Hat Enterprise Linux 10	A heap buffer overflow vulnerability was found in GStreamer's librfb (RFB/VNC client). The rectangle bounds check incorrectly validates area rather than individual dimensions, allowing a malicious VNC server to send a rectangle that extends beyond the framebuffer. A remote attacker could set up a malicious VNC server and trick a user into connecting, resulting in an out-of-bounds heap write that could lead to code execution or a crash.	2026-06-15	8.8	CVE-2026-52720
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in the cifs-utils package where the cifs.upcall helper fails to securely drop its root privileges before looking up user information inside a user-controlled environment. A local, low privileged attacker can exploit this by using a crafted request_key payload to trick the root-owned helper into entering a custom environment (namespace) containing a malicious NSS module. This forces the system to load the attacker's	2026-06-18	7.8	CVE-2026-12505

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	controlled NSS Module and configuration, allowing them to execute arbitrary commands as the root user, elevating their privileges and fully compromising the system.			
Red Hat--Red Hat Enterprise Linux 10	An out-of-bounds read vulnerability was found in the VA JPEG decoder in GStreamer's gst-plugins-bad. The JPEG parser reads a segment length value from the bitstream without validating it against available data. A remote attacker could trick a user into opening a specially crafted JPEG file, causing downstream parsing to read beyond the provided input buffer, leading to a crash or potential information disclosure.	2026-06-15	7.1	CVE-2026-52719
Red Hat--Red Hat Enterprise Linux 10	A signed integer overflow vulnerability was found in GStreamer's VMnc decoder. A crafted VMnc stream with large cursor dimensions can overflow signed integer payload-size arithmetic, bypassing a length check and leading to out-of-bounds reads. A remote attacker could trick a user into opening a specially crafted VMnc file, potentially causing a crash or information disclosure.	2026-06-15	7.1	CVE-2026-52722
Red Hat--Red Hat Enterprise Linux 10	A vulnerability was found in the GStreamer RealMedia demuxer (gst-plugins-ugly). When processing a RealMedia (.rm) file, the demuxer parses MDPD (media properties) chunks to configure audio streams. For audio stream header versions 4 and 5, the parser reads fields such as codec type, packet size, sample rate, channel count, and extra codec data length from fixed offsets within the chunk without first checking that the chunk contains enough data. If a malicious file provides an MDPD chunk that is too small to contain a complete audio stream header, the parser reads beyond the end of the buffer. This can cause the application to crash. In some cases, bytes read past the buffer boundary may be incorporated into stream metadata, which could result in limited information disclosure.	2026-06-15	7.1	CVE-2026-53703
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in GStreamer's RealMedia demuxer in the gst-plugins-ugly package. When processing a RealMedia file containing a specially crafted FILEINFO metadata section, the demuxer parses variable-name and variable-value pairs using re_skip_pascal_string() without validating that offsets remain within the mapped buffer. Additionally, the element count controlling the parsing loop is read from attacker-controlled data without validation, which can cause an infinite loop. A crafted RealMedia file can cause the application to crash, hang, or potentially read limited adjacent memory contents.	2026-06-15	7.1	CVE-2026-53704
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in GStreamer's WavPack audio decoder in gst-plugins-good. When processing a specially crafted WavPack file, an integer overflow in the buffer size calculation (4 * block_samples * channels) in gst_wavpack_dec_handle_frame() causes a very small heap allocation. The WavPack library then writes decoded audio samples far beyond the allocated buffer, resulting in heap memory corruption. This affects both 32-bit and 64-bit systems since the arithmetic is performed in 32-bit integers before promotion to the allocation size type. A remote attacker could use this flaw to crash an application or potentially execute arbitrary code by convincing a user to open a malicious WavPack audio file.	2026-06-15	7.6	CVE-2026-53705
Red Hat--Red Hat Enterprise Linux 10	A heap buffer overflow vulnerability was found in libaom, the reference AV1 codec implementation. A flaw in the AV1 encoder's Look-Ahead Processing (LAP) mode causes the first-pass stats ring buffer wrap-around guard to be bypassed when g_lag_in_frames is set to 1 or higher. This results in a 232-byte out-of-bounds write on every encoded frame after the second, corrupting adjacent heap objects. An attacker who can influence encoder configuration in a transcoding service or WebRTC session could exploit this to cause a denial of service (process crash) or potentially achieve code execution.	2026-06-19	7.6	CVE-2026-56208
Red Hat--Red Hat Enterprise Linux 10	An arbitrary address write vulnerability was found in libaom, the reference AV1 codec implementation. A missing bounds check in the SVC (Scalable Video Coding) layer ID control function allows an attacker to inject an arbitrary pointer into the cyclic refresh map field via crafted image pixel values. The encoder then writes approximately 1,200 bytes at the attacker-	2026-06-19	7.1	CVE-2026-56209

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	controlled address. This is fully deterministic and does not require a separate information leak. An attacker who can supply frames to a network-facing libaom encoder with SVC enabled could exploit this for denial of service or potential code execution.			
Red Hat--Red Hat Enterprise Linux 10	A heap-buffer-overflow read vulnerability was found in libaom, the reference AV1 codec implementation. A missing bounds check in the SVC (Scalable Video Coding) layer ID control function allows setting a spatial_layer_id exceeding the configured number of layers. This causes an out-of-bounds heap read of approximately 40,728 bytes when computing a layer context array index. An attacker who can influence SVC encoder parameters in a network-facing service could exploit this for information disclosure (heap content leak) or denial of service (segmentation fault from hitting unmapped memory).	2026-06-19	7.1	CVE-2026-56210
Red Hat--Red Hat Enterprise Linux 10	A remote code execution vulnerability was found in libaom, the reference AV1 codec implementation. Insufficient bounds validation in the AV1 encoder's SVC (Scalable Video Coding) layer ID control allows an attacker to supply crafted video frame pixels that overlap with internal encoder layer context structures. In fork-based video processing services, an attacker can use this to hijack the cyclic refresh map pointer, brute-force the process base address via a crash oracle, and redirect control flow to achieve arbitrary command execution. Exploitation requires the target service to use libaom with SVC encoding enabled and accept attacker-supplied video frames.	2026-06-19	7.1	CVE-2026-56211
Redhat--QEMU	A flaw was found in QEMU. When reading input audio in the virtio-snd device input callback, the `virtio_snd_pcm_in_cb` function did not check whether the iov could fit the data buffer, potentially leading to a heap out-of-bounds write. This issue exists due to an incomplete fix for CVE-2024-7730.	2026-06-19	7.4	CVE-2026-3195
RelyWP--Coupon Affiliates	Unauthenticated Cross Site Scripting (XSS) in Coupon Affiliates <= 7.5.3 versions.	2026-06-15	7.1	CVE-2026-40770
RelyWP--Coupon Affiliates	Subscriber Sensitive Data Exposure in Coupon Affiliates <= 7.8.1 versions.	2026-06-15	7.5	CVE-2026-49068
ReviewX--ReviewX	Unauthenticated Broken Authentication in ReviewX <= 2.3.6 versions.	2026-06-15	7.5	CVE-2026-40781
Ritlabs--TinyWeb Server	A security vulnerability has been detected in Ritlabs TinyWeb Server up to 1.94 on Win32. This impacts an unknown function in the library libeay32.dll.html of the component Header Handler. The manipulation of the argument Authorization leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	7.3	CVE-2026-12200
Royal Elementor Addons--Royal Elementor Addons Pro	Unauthenticated Cross Site Scripting (XSS) in Royal Elementor Addons Pro < 1.7.1041 versions.	2026-06-17	7.1	CVE-2026-40720
Royal Plugins--Royal MCP	Unauthenticated Broken Access Control in Royal MCP <= 1.4.2 versions.	2026-06-15	7.3	CVE-2026-40775
Ruben Garcia--AutomatorWP	Subscriber Broken Authentication in AutomatorWP <= 5.6.7 versions.	2026-06-15	7.1	CVE-2026-40785
Ruben Garcia--AutomatorWP	Unauthenticated Cross Site Scripting (XSS) in AutomatorWP <= 5.6.7 versions.	2026-06-15	7.2	CVE-2026-42650
Ruben Garcia--AutomatorWP	Unauthenticated Cross Site Scripting (XSS) in AutomatorWP <= 5.7.2 versions.	2026-06-15	7.1	CVE-2026-42775
Ruben Garcia--GamiPress	Subscriber SQL Injection in GamiPress <= 7.8.7 versions.	2026-06-15	8.5	CVE-2026-48874
rxii--microtar	A stack-based buffer overflow exists in the raw_to_header() function in src/microtar.c in rxii microtar 0.1.0. The function copies the 100-byte name and linkname fields of a TAR header with strcpy() without guaranteeing	2026-06-17	8.8	CVE-2026-55738

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	null termination of the source. The POSIX ustar format permits these fixed-width fields to be fully populated with non-null bytes, so a crafted archive whose linkname field (followed by the trailing padding of the 512-byte raw header) contains no null terminator causes strcpy() to read past the end of the 512-byte raw header stack buffer and to write past the destination header buffer. A remote attacker who supplies a crafted TAR archive that the victim opens or parses (via mtar_open(), mtar_read_header(), or mtar_find()) can cause an out-of-bounds read and a stack buffer overflow, resulting in denial of service (crash) and potentially arbitrary code execution. Confirmed with AddressSanitizer: stack-buffer-overflow READ of size 356 in raw_to_header at src/microtar.c:112.			
rxii--microtar	An integer overflow in the mtar_next() function in src/microtar.c in rxii microtar 0.1.0 allows a remote attacker to cause a denial of service (uncontrolled CPU consumption / infinite loop) via a crafted tar archive. mtar_next() computes the offset to the next record as round_up(h.size, 512) + sizeof(mtar_raw_header_t) using 32-bit arithmetic. When the header size field is a multiple of 512 in the range 0xFFFFFC01-0xFFFFFE00 (e.g. 0xFFFFFE00), the addition wraps to 0, so mtar_next() seeks to the current record position instead of advancing. As a result, mtar_find() and any loop that iterates entries with mtar_next() repeat indefinitely over the same record, hanging the process at 100% CPU with no recovery.	2026-06-17	7.5	CVE-2026-54417
SaaSProject--Booking Package	Unauthenticated Broken Access Control in Booking Package <= 1.7.06 versions.	2026-06-15	7.5	CVE-2026-40774
Satinder Singh--Contact Form Extender for Divi Save Entries, File Upload & Country Code Field	Unauthenticated Arbitrary File Deletion in Contact Form Extender for Divi Save Entries, File Upload & Country Code Field <= 1.0.6 versions.	2026-06-15	8.6	CVE-2026-40769
sbouey--Falang multilanguage	Subscriber Privilege Escalation in Falang multilanguage <= 1.4.2 versions.	2026-06-17	8.8	CVE-2026-54805
Schiocco--Support Board	Unauthenticated Privilege Escalation in Support Board < 3.8.9 versions.	2026-06-16	9.8	CVE-2026-27395
Select-Themes--Getaway	Unauthenticated Local File Inclusion in Getaway < 1.8 versions.	2026-06-16	8.1	CVE-2026-39547
Select-Themes--Hiroshi	Unauthenticated PHP Object Injection in Hiroshi <= 1.5.1 versions.	2026-06-17	8.1	CVE-2026-39560
Select-Themes--Manufaktur Solutions	Unauthenticated PHP Object Injection in Manufaktur Solutions <= 1.1.1 versions.	2026-06-17	8.1	CVE-2026-40752
Select-Themes--Micdrop	Unauthenticated PHP Object Injection in Micdrop <= 1.3.1 versions.	2026-06-16	8.1	CVE-2026-39580
Select-Themes--Mildhill	Unauthenticated PHP Object Injection in Mildhill <= 1.5 versions.	2026-06-17	8.1	CVE-2026-39573
Select-Themes--Sant	Unauthenticated PHP Object Injection in SantÃ© <= 1.5.1 versions.	2026-06-16	8.1	CVE-2026-39567
Select-Themes--Zermatt	Unauthenticated PHP Object Injection in Zermatt <= 1.6.1 versions.	2026-06-17	8.1	CVE-2026-39545
sentriz--gonic	gonic is a music streaming server / free-software subsonic server API implementation. Prior to version 0.21.0, a logic error in 'ServeCreateOrUpdatePlaylist' allows any authenticated Subsonic user (including non-admin) to write playlist M3U content to an attacker-controlled absolute filesystem path on the gonic host, and to create intermediate directories with '0o777' permissions. The bug is independent of CVE-2026-49338 and CVE-2026-49339. It is an unreachable guard clause combined with no path containment in 'Store.Write'. Version 0.21.0 patches the issue.	2026-06-19	8.1	CVE-2026-49340

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sentriz--gonic	gonic is a music streaming server / free-software subsonic server API implementation. Prior to version 0.21.0, the Subsonic API endpoints `/rest/deletePlaylist.view` and `/rest/getPlaylist.view` perform no per-resource authorization. Once authenticated as any user (admin or not), an attacker can delete any playlist owned by any other user (including admin) by passing its `id` and read the full contents (name, comment, song list) of any other user's **private** (non-public) playlist by passing its `id`. The Subsonic playlist `id` is `base64url("<userID>/<filename>.m3u")`. Because filenames are user-supplied or time-derived and the `userID` is a small integer, IDs are guessable and frequently exposed (e.g. a previously-public playlist that was later made private still has the same ID). This breaks the multi-user trust boundary of gonic: a low-privileged user can wipe an administrator's curated playlists, and a user can exfiltrate any private playlist they obtain an ID for. The issue was fixed in commit `6dd71e6a3c966867ef8c900d359a7df75789f410`, which is part of version 0.21.0.	2026-06-19	7.1	CVE-2026-49338
sentriz--gonic	gonic is a music streaming server / free-software subsonic server API implementation. The maintainer's fix in commit `6dd71e6a3c966867ef8c900d359a7df75789f410` added an ownership check based on `playlist.UserID`. However, `playlist.UserID` is derived from the first path segment of the attacker-controlled playlist ID, with no path containment on the resolved file path. Any authenticated Subsonic user can therefore bypass the ownership check and read any other user's playlist, delete any other user's playlist, and probe arbitrary file paths on the host for existence/readability. This is a bypass of the boundary the `6dd71e6` fix is trying to enforce; it is closely related to the original GONIC-1 IDOR but uses a different primitive (path traversal in the `id` parameter rather than direct cross-user access). Commit 0824bed88f6bbcb490ba28bf09d28e5dfef07b445 in version 0.21.0 fixes the issue.	2026-06-19	7.1	CVE-2026-49339
SEO Squirrly--SEO Plugin by Squirrly SEO	Unauthenticated Broken Access Control in SEO Plugin by Squirrly SEO <= 12.4.16 versions.	2026-06-16	7.5	CVE-2026-52714
ServerCo--getssl	In ServerCo getssl version 2.49 and prior, the ACME challenge token returned to the client was not strictly validated against RFC 8555 before being used in challenge-file handling, allowing a maliciously crafted token to influence local path/filename usage during validation. An attacker who can supply ACME challenge responses to getssl (for example, a malicious or compromised CA endpoint, or an on-path adversary able to tamper with that response path) could exploit this to achieve unauthorized file write/path traversal effects, usually with elevated privileges, ultimately allowing for remote command injection. This issue appears related in spirit to CVE-2023-38198, and is an instance of CWE-73, "External control of file name or path." Other ACME shell script handlers may be affected by similar issues.	2026-06-16	7.4	CVE-2026-10303
SeventhQueen--SweetDate Core	Unauthenticated Cross Site Scripting (XSS) in SweetDate Core < 1.1.5 versions.	2026-06-17	7.1	CVE-2025-69140
Shipster--Baggage Freight Shipping Australia	WordPress Plugin Baggage Freight Shipping Australia 0.1.0 contains an unrestricted file upload vulnerability that allows unauthenticated attackers to upload arbitrary files by exploiting the upload-package.php endpoint. Attackers can submit POST requests with malicious file extensions to the upload handler, which moves files without validation to the plugin upload directory, enabling remote code execution.	2026-06-15	9.8	CVE-2018-25436
ShopXO--ShopXO	A vulnerability was determined in ShopXO up to 6.7.1. This vulnerability affects the function OrderClose/OrderSuccess/PayLogOrderClose/GoodsGiveIntegral of the file app/api/controller/Crontab.php of the component Scheduled Task Endpoint. Executing a manipulation can lead to authorization bypass. The attack can be executed remotely. The exploit has been publicly disclosed	2026-06-15	7.3	CVE-2026-12204

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.			
ShortPixel--ShortPixel Image Optimizer	Author PHP Object Injection in ShortPixel Image Optimizer <= 6.4.3 versions.	2026-06-15	7.2	CVE-2026-39471
Significant-Gravitas--AutoGPT	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. Versions prior to 0.6.62 have a DOM-based Cross-Site Scripting (XSS) vulnerability in AutoGPT's signup page. The application improperly trusts a URL parameter ('next'), which is passed to 'router.push'. An attacker can craft a malicious link that, when opened by an authenticated user, performs a client-side redirect and executes arbitrary JavaScript in the context of their browser. This could lead to credential theft, internal network pivoting, and unauthorized actions performed on behalf of the victim. Version 0.6.62 patches the issue.	2026-06-18	8.8	CVE-2026-55237
Simbunch--SIMGenealogy	Joomla! Component SIMGenealogy 2.1.5 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the type parameter. Attackers can send GET requests to index.php with the option=com_simgenealogy, view=latest parameters and inject malicious SQL in the type parameter to extract sensitive database information.	2026-06-19	8.2	CVE-2017-20276
SiYuan--SiYuan	SiYuan before v3.6.1 fails to sanitize package metadata and README content in the Bazaar marketplace, allowing malicious package authors to inject arbitrary HTML and JavaScript. Attackers can achieve remote code execution on any user browsing the Bazaar by embedding XSS payloads in package displayName, description, or README fields, exploiting Electron's nodeIntegration setting to execute OS commands.	2026-06-21	9.6	CVE-2026-56395
SiYuan--SiYuan	SiYuan before v3.6.1 fails to sanitize package metadata and README content in the Bazaar marketplace, allowing malicious package authors to inject arbitrary HTML and JavaScript. Attackers can achieve remote code execution on any user browsing the Bazaar by embedding XSS payloads in package displayName, description, or README fields, exploiting Electron's nodeIntegration setting to execute OS commands.	2026-06-21	9.6	CVE-2026-56397
SlicedInvoices--Sliced Invoices	WordPress Sliced Invoices 3.8.2 contains an authenticated SQL injection vulnerability that allows authenticated attackers to manipulate database queries by injecting SQL code through the 'post' parameter. Attackers can send requests to the admin.php endpoint with action=duplicate_quote_invoice and malicious 'post' values to extract sensitive database information or modify data.	2026-06-15	7.1	CVE-2019-25746
Sneeiit--MagOne	Unauthenticated Cross Site Scripting (XSS) in MagOne <= 9.0 versions.	2026-06-16	7.1	CVE-2026-39548
Soft-Php--jCart for OpenCart	Joomla! Component jCart for OpenCart 2.0 contains an SQL injection vulnerability that allows unauthenticated attackers to manipulate database queries by injecting SQL code through the product_id parameter. Attackers can send GET requests to index.php with the option=com_jcart&route=product/product parameters and malicious product_id values to extract sensitive database information.	2026-06-19	8.2	CVE-2017-20282
SONAAR MUSIC--Sonaar	Subscriber Privilege Escalation in Sonaar <= 4.27.4 versions.	2026-06-17	8.8	CVE-2025-59563
SONAAR MUSIC--Sonaar	Unauthenticated Cross Site Scripting (XSS) in Sonaar <= 4.27.4 versions.	2026-06-17	7.1	CVE-2025-59560
SourceCodester--CET Automated Grading System with AI Predictive Analytics	A security vulnerability has been detected in SourceCodester CET Automated Grading System with AI Predictive Analytics 1.0. Affected is an unknown function of the file /index.php of the component Student Self-Registration Endpoint. The manipulation leads to improper access controls. Remote exploitation of the attack is possible.	2026-06-17	7.3	CVE-2026-12529

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SpeakOut!-- SpeakOut! Email Petitions	Unauthenticated SQL Injection in SpeakOut! Email Petitions <= 4.6.5 versions.	2026-06-15	9.3	CVE-2026-39530
Splunk--Splunk AI Toolkit	In Splunk AI Toolkit versions below 5.7.4, a user who holds the "admin" Splunk role could execute arbitrary OS commands on the host running the Splunk Enterprise instance. The vulnerability is possible because of an unsafe shell execution pattern in the btool configuration helper, which constructs OS command strings from dynamic parameters without disabling shell interpretation.	2026-06-17	9.1	CVE-2026-20266
Spring--Spring AI	In Spring AI Vector Stores, special characters could be used to force the execution of arbitrary queries in Elasticsearch, OpenSearch, and GemFire VectorDB. Affected components: spring-ai-elasticsearch-store, spring-ai-opensearch-store, spring-ai-gemfire-store. Affected versions: Spring AI 1.0.0 through 1.0.x (fix 1.0.9). Spring AI 1.1.0 through 1.1.x (fix 1.1.8).	2026-06-15	8.6	CVE-2026-47835
Spring--Spring Cloud Gateway	Spring Cloud Gateway Server forwards the X-Forwarded-For and Forwarded headers from untrusted proxies in certain configuration scenarios. This affects both the WebMVC and WebFlux Gateway Servers. Affected versions: Spring Cloud Gateway 3.1.x (fix 3.1.13). Spring Cloud Gateway 4.1.x (fix 4.1.13). Spring Cloud Gateway 4.2.x (fix 4.2.9). Spring Cloud Gateway 4.3.x (fix 4.3.5). Spring Cloud Gateway 5.0.x (fix 5.0.2).	2026-06-15	8.6	CVE-2026-47825
Spring--Spring Cloud Sleuth	In Spring Cloud Sleuth, it is possible for a user to provide specially crafted calls that may cause a denial-of-service (DoS) condition. The application is vulnerable when it uses a vulnerable version of org.springframework.cloud:spring-cloud-sleuth-instrumentation and Spring TX instrumentation is not disabled. Affected versions: Spring Cloud Sleuth 3.1.0 through 3.1.13.	2026-06-15	7.5	CVE-2026-41708
startreedata--mcp-pinot	mcp-pinot is a Python-based Model Context Protocol (MCP) server for interacting with Apache Pinot. In versions 3.0.1 and below, mcp-pinot defaults to running an HTTP MCP server bound to 0.0.0.0:8080 with no authentication enabled. All MCP tools, including SQL query execution, schema creation, and table-config mutation, are reachable by any network-adjacent caller. The server proxies these calls using server-side Pinot credentials, producing a confused-deputy condition that yields full read/write access to the configured Pinot cluster. This issue has been fixed in version 3.1.0	2026-06-18	10	CVE-2026-49257
statamic--cms	Statamic is a Laravel and Git powered content management system (CMS). Prior to 5.73.23 and 6.20.0, the fix for CVE-2026-41175 was incomplete. It addressed the issue in the query builder, but the same protection was not applied to in-memory collection sorting. Manipulating sort parameters could result in the loss of content and assets. This requires a front-end template that passes request input into a tag's sort parameter. It is not exploitable by default - a template would need to be explicitly set up to sort by a visitor-controlled value. This has been fixed in 5.73.23 and 6.20.0.	2026-06-19	7.4	CVE-2026-49287
SteeltoeOSS--Steeltoe.Discovery.Eureka	Steeltoe is an open source project that provides a collection of libraries that helps users build cloud-native applications. In Steeltoe.Discovery.Eureka prior to versions 4.2.0 and 3.4.0, `DataCenterInfo.FromJson` throws `ArgumentException` for any `name` value other than `"MyOwn"` or `"Amazon"`, despite the Java Eureka specification defining a third valid value: `"Netflix"`. The exception propagates through the entire registry deserialization chain and is swallowed by the periodic cache refresh task, leaving the local service registry permanently empty or stale. Versions 4.2.0 and 3.4.0 patch the issue. If an immediate upgrade is not possible, remove any registrations using unsupported `DataCenterInfo.name` values from the registry. In mixed Java/Spring and Steeltoe environments, audit for the `Netflix` data center type before deploying Steeltoe Eureka clients.	2026-06-17	7.5	CVE-2026-50196
SteeltoeOSS--Steeltoe.Management.Endpoint	Steeltoe is an open source project that provides a collection of libraries that helps users build cloud-native applications. When Steeltoe management endpoints versions 3.2.2 through 3.3.0 and 4.1.0 are	2026-06-17	8.2	CVE-2026-50194

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	configured to listen on an alternate port (`Management:Endpoints:Port` is configured), the middleware responsible for restricting access to the endpoints uses the `Host` HTTP header rather than the actual network socket port. Versions 3.4.0 and 4.2.0 patch the issue. If an immediate upgrade to a patched version is not possible, add explicit ASP.NET Core authorization (`RequireAuthorization`) to all sensitive actuator endpoints as a defense-in-depth measure independent of port isolation and/or configure the reverse proxy or load balancer to enforce the `Host` header value and prevent clients from setting an arbitrary port.			
SteeltoeOSS--Steeltoe.Management.Endpoint	Steeltoe is an open source project that provides a collection of libraries that helps users build cloud-native applications. In Steeltoe.Management.Endpoint prior to version 4.2.0 and Steeltoe.Management.EndpointCore prior to version 3.4.0, the `Sanitizer` component in the Environment actuator redacts configuration values by matching the configuration key name against a suffix list. The default list (`password`, `secret`, `key`, `token`, `.*credentials.*`, `vcap_services`) does not cover the standard .NET pattern `ConnectionStrings:<name>` or Steeltoe Connectors' `Steeltoe:Client:<type>:Default:ConnectionString`. There is no value-based scrubbing, so full connection string values including embedded `Password=` and `user:pass@host` segments are returned verbatim in `/actuator/env` responses. Steeltoe.Management.Endpoint 4.2.0 and Steeltoe.Management.EndpointCore 3.4.0 patch the issue. If an immediate upgrade is not possible: On the standard path, remove `env` from the actuator exposure list; add `.*connectionstring.*` to `KeysToSanitize` as a defense-in-depth measure for both paths; and/or require authorization on actuator endpoints.	2026-06-17	7.5	CVE-2026-50200
Stiofan--Events Calendar for GeoDirectory	Contributor PHP Object Injection in Events Calendar for GeoDirectory <= 2.3.25 versions.	2026-06-15	8.8	CVE-2026-39532
Stiofan--GetPaid	Insertion of Sensitive Information Into Sent Data vulnerability in Stiofan GetPaid allows Retrieve Embedded Sensitive Data. This issue affects GetPaid: from n/a through 2.8.49.	2026-06-15	7.5	CVE-2026-49064
strukturag--libde265	libde265 is an open source implementation of the h.265 video codec. Prior to version 1.0.20, a crafted H.265 bitstream can cause an out-of-bounds array write in `decoder_context::process_reference_picture_set()` (`libde265/decctx.cc:1376`). The root cause is a missing aggregate bound check on predicted short-term reference picture set entries. Individual list sizes are validated, but the combined count after predicted RPS construction can exceed the 16-entry `PocStFoll` array, writing at index 16. Version 1.0.20 patches the issue.	2026-06-19	7.1	CVE-2026-49295
strukturag--libde265	libde265 is an open source implementation of the h.265 video codec. Prior to version 1.1.0, a crafted H.265 bitstream with large SPS dimensions and 16-bit bit depth causes a signed integer overflow in `de265_image_get_buffer()` (`libde265/image.cc:128`). The overflow wraps the plane allocation size to a small value (~1 KB), but the subsequent `fill_image()` call computes the real size using `size_t`, writing ~4 GB into the undersized heap buffer. Version 1.1.0 patches the issue.	2026-06-19	7.1	CVE-2026-49346
Studio Keren Aga LTD.--Unlimited Elements for Elementor (Premium)	Contributor Arbitrary File Upload in Unlimited Elements for Elementor (Premium) <= 2.0.6 versions.	2026-06-17	9.9	CVE-2026-27041
StylemixThemes--MasterStudy LMS	Subscriber SQL Injection in MasterStudy LMS <= 3.7.25 versions.	2026-06-15	8.5	CVE-2026-40766
StylemixThemes--Motors	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in StylemixThemes Motors allows Blind SQL Injection. This issue affects Motors: from n/a through 1.4.109.	2026-06-17	9.3	CVE-2026-54812

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
StylemixThemes--Motors	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in StylemixThemes Motors allows PHP Local File Inclusion. This issue affects Motors: from n/a through 1.4.109.	2026-06-17	8.1	CVE-2026-54814
sunnyadn--js-toml	js-toml is a TOML parser for JavaScript, fully compliant with the TOML 1.0.0 Spec. Versions up to and including 1.1.0 parse hexadecimal / octal / binary integer literals via a hand-written `parseBigInt` loop that multiplies a `BigInt` accumulator by the radix once per input digit. Each iteration performs a `BigInt * BigInt` operation on an accumulator that grows linearly with the number of digits already consumed, so the whole loop is $O(n^2)$ in the literal length. The lexer regex places no upper bound on the literal length, so a single TOML document containing one ~500 kB hex literal pins one CPU core for ~40 seconds on a modern laptop (Apple M-series, Node v22). Memory amplification is bounded but CPU amplification is severe and grows quadratically: doubling the literal length quadruples the work. A caller that invokes `load()` on attacker-controlled TOML (configuration upload endpoints, CI/CD systems ingesting third-party `*.toml`, IDE plugins, build tools) is exposed to a single-request CPU exhaustion DoS. Version 1.1.1 fixes the issue.	2026-06-19	7.5	CVE-2026-49293
SUSE--Harvester	An attacker with network-level access between the SUSE Virtualization and Rancher Manager in SUSE Harvester before 1.8.0 could interfere with the TLS handshake and abuse it to bypass TLS as a security control.	2026-06-16	8.6	CVE-2025-71261
SUSE--wicked	Passing of unsanitized strings from DHCP replies into the wicked dhcp client before wicked 0.6.79 could be used by attackers operating a malicious DHCP server to execute code on the local machine.	2026-06-16	8.8	CVE-2026-44932
Syed Balkhi--PushEngage Web Push Notifications, eCommerce Automation & Chat Widget	Subscriber Sensitive Data Exposure in PushEngage - Web Push Notifications, eCommerce Automation & Chat Widget <= 4.2.3 versions.	2026-06-17	7.4	CVE-2026-52698
Sync-in--server	Sync-in Server is a secure, open-source platform for file storage, sharing, collaboration, and syncing. Prior to version 2.3.0, the private IP blocklist regex used in the URL download feature does not match IPv4-mapped IPv6 addresses (e.g. ::ffff:127.0.0.1), allowing SSRF protection to be bypassed on dual-stack systems. Version 2.3.0 fixes the issue.	2026-06-16	7.7	CVE-2026-47684
sysown--proxysql	ProxySQL is a proxy for MySQL and its forks, as well as PostgreSQL. In versions 2.0.0 through 3.0.8, the ProxySQL MySQL frontend accepts the `PROXY UNKNOWN <addr> <addr> <port> <port>\r\n` PP1 frame as a well-formed PROXY protocol header. The HAProxy PROXY protocol v1 specification says that when the protocol token is `UNKNOWN`, the receiver MUST ignore any address fields that follow it, because the proxy has declared it cannot determine the client identity. ProxySQL parses those address fields anyway via `sscanf` and writes the spoofed source address into the session's `addr.addr` field. From there it flows directly into the query-rule matcher, where the `client_addr` predicate decides routing and ACL. When `mysql-proxy_protocol_networks = '*'` (the default), any TCP peer can send a PP1 frame and choose any source IP claim. With that, any `mysql_query_rules` row pinned to a `client_addr` value is forgeable: the attacker writes the address they want to match into the PP1 line, and ProxySQL routes their query as if it came from that address. In practice this is a routing and ACL bypass. Real deployments use `client_addr` for read-write splitting (internal apps go to the primary, public traffic to read replicas), per-app schema pinning, and query-filter rules (DDL allowed only from admin CIDR, public queries blocked from dangerous patterns). An attacker that can reach the frontend port can forge their way into any of those routes. Version 3.0.9 patches this issue.	2026-06-19	10	CVE-2026-48772

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sysown--proxysql	ProxySQL is a proxy for MySQL and its forks, as well as PostgreSQL. Versions 2.0.18 through 3.0.8 have a pre-authentication heap memory corruption vulnerability in the MySQL and PostgreSQL protocol first-read paths. A remote unauthenticated client can declare an oversized first packet length, and ProxySQL passes that attacker-controlled length directly to `recv()` while writing into a fixed 32 KB input queue. Version 3.0.9 patches the issue.	2026-06-19	9.8	CVE-2026-48773
sysown--proxysql	ProxySQL is a proxy for MySQL and its forks, as well as PostgreSQL. In versions 3.0.0 through 3.0.8, ProxySQL's GenAI/MCP `run_sql_readonly` tool violates its documented read-only contract for MySQL targets. The tool validates only the full input string with a substring blacklist and first-keyword allowlist, but then executes the entire SQL string on a backend connection created with `CLIENT_MULTI_STATEMENTS`. As a result, a caller can submit a read-only first statement followed by a side-effecting second statement, such as `SELECT 1; RENAME TABLE ...`. The validator accepts the payload because it starts with `SELECT` and because side-effecting MySQL statements such as `RENAME TABLE`, `SET`, `RESET`, `LOCK TABLES`, and `KILL` are not rejected by the blacklist. In a live MCP runtime test, the `/mcp/query` endpoint accepted a `run_sql_readonly` request. The MCP response reported success for the first `SELECT`, and direct backend verification showed that the table had actually been renamed. This violates the endpoint's read-only security contract and lets an MCP caller perform backend writes or administrative SQL, limited by the configured MCP target account's database privileges. Version 3.0.9 contains a fix. Other operator mitigations include: keeping MCP disabled unless required; setting a non-empty `mcp-query_endpoint_auth` token before exposing `/mcp/query`; restricting MCP listener network exposure; configuring MCP backend target credentials as database-level read-only users; and adding temporary MCP query rules to block obvious multi-statement patterns.	2026-06-19	7.5	CVE-2026-48774
szTheory--relyra	Relyra is a strict-by-default SAML 2.0 Service Provider library for Elixir and Phoenix. Versions 1.0.0 and 1.1.0 accept forged SAML signatures because SignatureValue was not cryptographically verified before the library returned a successful authentication result. The XMLDSig trust boundary was incomplete as :public_key.verify over the exclusive-C14N canonicalized SignedInfo was not performed against the configured IdP certificate's public key, DigestValue was not recomputed over the canonicalized referenced element, and canonicalize/2 remained an unused passthrough in the signature-verification path. The result was a structure-only acceptance path where document shape and trust-source rejection could succeed without proving the signature bytes. A forged SignatureValue carrying an attacker-controlled NameID could be accepted as {:ok}. This issue has been fixed in version 1.2.0.	2026-06-18	9.1	CVE-2026-49454
Takashi Kitajima--MW WP Form	Unauthenticated Cross Site Scripting (XSS) in MW WP Form <= 5.1.3 versions.	2026-06-15	7.1	CVE-2026-48871
Tammersoft--Shared Files	Unauthenticated Path Traversal in Shared Files <= 1.7.64 versions.	2026-06-15	7.5	CVE-2026-49112
Taskbuilder--Taskbuilder	Subscriber SQL Injection in Taskbuilder <= 5.0.7 versions.	2026-06-15	8.5	CVE-2026-52697
Techspawn--MultiLoca	Subscriber Privilege Escalation in MultiLoca <= 4.2.15 versions.	2026-06-17	7.6	CVE-2026-39546
Terrywcarter--KissGallery	Joomla! Component KissGallery 1.0.0 contains an SQL injection vulnerability that allows unauthenticated attackers to inject SQL commands through the component URL path. Attackers can supply malicious SQL code in the kissgallery endpoint to execute arbitrary database queries and extract sensitive information.	2026-06-19	8.2	CVE-2017-20269
The Browser Company of New York--Arc Search	Address bar spoofing in Arc Search for Android allows a remote attacker to display a trusted domain in the address bar while rendering attacker-controlled content, enabling phishing.	2026-06-16	7.4	CVE-2026-12348

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
themagnifico52--Charity Zone	Subscriber Arbitrary File Upload in Charity Zone <= 1.1.1 versions.	2026-06-17	9.9	CVE-2026-40749
themagnifico52--Ecommerce Zone	Subscriber Arbitrary File Upload in Ecommerce Zone <= 0.9.7 versions.	2026-06-17	9.9	CVE-2026-40747
themagnifico52--Kids Gift Shop	Subscriber Arbitrary File Upload in Kids Gift Shop <= 0.5.4 versions.	2026-06-17	9.9	CVE-2026-40748
themagnifico52--Kids Online Store	Unrestricted Upload of File with Dangerous Type vulnerability in themagnifico52 Kids Online Store allows Upload a Web Shell to a Web Server. This issue affects Kids Online Store: from n/a through 0.8.9.	2026-06-16	9.9	CVE-2026-40750
themagnifico52--Restaurant Zone	Subscriber Arbitrary File Upload in Restaurant Zone <= 0.7.8 versions.	2026-06-17	9.9	CVE-2026-40746
Theme passion--Support Ticket Management System	Unauthenticated Privilege Escalation in Support Ticket Management System <= 1.9 versions.	2026-06-17	9.8	CVE-2025-69179
THEMECO--Cornerstone	Subscriber Arbitrary Code Execution in Cornerstone < 7.8.8 versions.	2026-06-16	8.5	CVE-2026-49113
THEMECO--Cornerstone	Subscriber SQL Injection in Cornerstone < 7.8.8 versions.	2026-06-17	8.5	CVE-2026-54185
ThemeFusion--Avada	Contributor PHP Object Injection in Avada <= 3.15.3 versions.	2026-06-16	8.8	CVE-2026-12256
themefusion--Avada (Fusion) Builder	The Avada (Fusion) Builder plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the maybe_delete_files function in all versions up to, and including, 3.15.3. This makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). The attack requires a published Avada form configured to save entries to the database; an unauthenticated attacker submits a path-traversal payload via the wp_ajax_nopriv_fusion_form_submit_ajax handler while also controlling the fusion_privacy_expiration_interval and privacy_expiration_action fields to force an immediate 'delete' cleanup, causing the planted entry to be automatically processed by the Fusion_Form_DB_Privacy shutdown-hook routine without any administrator interaction.	2026-06-19	9.1	CVE-2026-8713
ThemeFusion--Fusion Builder	Contributor PHP Object Injection in Fusion Builder <= 3.15.4 versions.	2026-06-16	9.8	CVE-2026-54194
ThemeFusion--Fusion Builder	Contributor Arbitrary File Deletion in Fusion Builder <= 3.15.4 versions.	2026-06-17	7.7	CVE-2026-54193
ThemeGoods--Avante	Unauthenticated Cross Site Scripting (XSS) in Avante < 3.0.5 versions.	2026-06-17	7.1	CVE-2025-68524
ThemeGoods--Grand Car Rental	Unauthenticated Cross Site Scripting (XSS) in Grand Car Rental <= 3.7 versions.	2026-06-16	7.1	CVE-2025-69151
ThemeGrill--Masteriyo - LMS	Incorrect Privilege Assignment vulnerability in ThemeGrill Masteriyo - LMS allows Privilege Escalation. This issue affects Masteriyo - LMS: from n/a through 2.2.0.	2026-06-15	8.8	CVE-2026-49111
ThemeGrill--Masteriyo - LMS	Unauthenticated Broken Access Control in Masteriyo - LMS <= 2.1.5 versions.	2026-06-15	7.5	CVE-2026-39524
ThemeGrill--Registration Form for WooCommerce	Unauthenticated Privilege Escalation in Registration Form for WooCommerce <= 1.0.9 versions.	2026-06-17	9.8	CVE-2026-54807
ThemeGrill--User Registration	Unauthenticated Broken Access Control in User Registration <= 5.1.2 versions.	2026-06-15	7.5	CVE-2026-25425
ThemeGrill--User Registration Stripe	Unauthenticated Broken Access Control in User Registration Stripe <= 1.3.14 versions.	2026-06-17	8.2	CVE-2026-40726

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ThemeGrill--User Registration Stripe	Unauthenticated Broken Access Control in User Registration Stripe <= 1.3.12 versions.	2026-06-17	8.2	CVE-2026-49081
Themeisle--Redirection for Contact Form 7	Unauthenticated Cross Site Scripting (XSS) in Redirection for Contact Form 7 <= 3.2.8 versions.	2026-06-15	7.1	CVE-2026-23970
Themeisle--Social Slider Feed	Unauthenticated Cross Site Scripting (XSS) in Social Slider Feed <= 2.3.2 versions.	2026-06-15	7.1	CVE-2026-39507
THEMELOGI--Roneous	Unauthenticated Local File Inclusion in Roneous <= 2.1.5 versions.	2026-06-16	8.1	CVE-2025-69177
THEMELOGI--Wanium	Unauthenticated Local File Inclusion in Wanium <= 1.9.8 versions.	2026-06-16	8.1	CVE-2025-69136
ThemeMove--Atomlab	Unauthenticated Local File Inclusion in Atomlab <= 2.4.5 versions.	2026-06-17	8.1	CVE-2026-39590
ThemeREX Group--Elementra	Unauthenticated PHP Object Injection in Elementra <= 1.0.9 versions.	2026-06-16	9.8	CVE-2026-39529
ThemeREX Group--Geya	Unauthenticated Local File Inclusion in Geya <= 1.15 versions.	2026-06-16	8.1	CVE-2025-58924
ThemeREX Group--Learnify	Unauthenticated Local File Inclusion in Learnify <= 1.15.0 versions.	2026-06-16	8.1	CVE-2025-60085
ThemeREX--Abelle	Unauthenticated Local File Inclusion in Abelle <= 1.22 versions.	2026-06-16	8.1	CVE-2025-69142
ThemeREX--AirSupply	Unauthenticated Local File Inclusion in AirSupply <= 2.0.0 versions.	2026-06-17	8.1	CVE-2025-69110
ThemeREX--AutoParts	Unauthenticated Local File Inclusion in AutoParts <= 1.5.8 versions.	2026-06-17	8.1	CVE-2026-22331
ThemeREX--Choreo	Unauthenticated Local File Inclusion in Choreo <= 1.6 versions.	2026-06-16	8.1	CVE-2025-69165
ThemeREX--CopyPress	Unauthenticated Local File Inclusion in CopyPress <= 1.4.5 versions.	2026-06-16	8.1	CVE-2025-69118
ThemeREX--Corbesier	Unauthenticated Local File Inclusion in Corbesier <= 1.15.0 versions.	2026-06-16	8.1	CVE-2025-69119
ThemeREX--Dazzle	Unauthenticated Local File Inclusion in Dazzle <= 1.0.0 versions.	2026-06-17	8.1	CVE-2025-69120
ThemeREX--Deliciosa	Unauthenticated Local File Inclusion in Deliciosa <= 1.10.0 versions.	2026-06-16	8.1	CVE-2025-69121
ThemeREX--Dom	Unauthenticated Local File Inclusion in Dom <= 1.24 versions.	2026-06-16	8.1	CVE-2025-69146
ThemeREX--EcoBlue	Unauthenticated Local File Inclusion in EcoBlue <= 1.15 versions.	2026-06-17	8.1	CVE-2026-22338
ThemeREX--Eros	Unauthenticated Local File Inclusion in Eros <= 1.3 versions.	2026-06-16	8.1	CVE-2025-69167
ThemeREX--Especio	Unauthenticated Local File Inclusion in Especio <= 1.0 versions.	2026-06-16	8.1	CVE-2025-69124
ThemeREX--Etude	Unauthenticated Local File Inclusion in Etude <= 1.6 versions.	2026-06-17	8.1	CVE-2025-69174
ThemeREX--Eventicity	Unauthenticated Local File Inclusion in Eventicity <= 1.5 versions.	2026-06-17	8.1	CVE-2025-69170
ThemeREX--Food Drop	Unauthenticated Local File Inclusion in Food Drop <= 1.3 versions.	2026-06-16	8.1	CVE-2025-69125
ThemeREX--Fortius	Unauthenticated Local File Inclusion in Fortius <= 2.3.0 versions.	2026-06-17	8.1	CVE-2025-69126
ThemeREX--Gamic	Unauthenticated Local File Inclusion in Gamic <= 1.15 versions.	2026-06-17	8.1	CVE-2025-69157
ThemeREX--Gat	Unauthenticated Local File Inclusion in Gat <= 1.16 versions.	2026-06-17	8.1	CVE-2025-69145

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ThemeREX--Gita	Unauthenticated Local File Inclusion in Gita <= 1.11 versions.	2026-06-16	8.1	CVE-2025-69160
ThemeREX--Granola	Unauthenticated Local File Inclusion in Granola <= 1.13 versions.	2026-06-17	8.1	CVE-2025-69158
ThemeREX--Grecko	Unauthenticated Local File Inclusion in Grecko <= 5.17 versions.	2026-06-16	8.1	CVE-2025-69162
ThemeREX--Gunslinger	Unauthenticated Local File Inclusion in Gunslinger <= 1.7 versions.	2026-06-17	8.1	CVE-2025-69166
ThemeREX--HomeRoofer	Unauthenticated Local File Inclusion in HomeRoofer <= 2.11.0 versions.	2026-06-17	8.1	CVE-2025-58954
ThemeREX--Hot Coffee	Unauthenticated PHP Object Injection in Hot Coffee <= 1.7 versions.	2026-06-16	9.8	CVE-2025-69108
ThemeREX--Imba	Unauthenticated Local File Inclusion in Imba <= 1.5.0 versions.	2026-06-17	8.1	CVE-2025-69106
ThemeREX--Ingenioso	Unauthenticated Local File Inclusion in Ingenioso <= 1.14.0 versions.	2026-06-17	8.1	CVE-2025-69117
ThemeREX--Iona	Unauthenticated Local File Inclusion in Iona <= 1.0.8 versions.	2026-06-16	8.1	CVE-2025-69116
ThemeREX--ITactics	Unauthenticated Local File Inclusion in ITactics <= 1.0 versions.	2026-06-16	8.1	CVE-2025-69176
ThemeREX--Joly	Unauthenticated Local File Inclusion in Joly <= 1.22.0 versions.	2026-06-17	8.1	CVE-2025-58953
ThemeREX--Kelly Young	Unauthenticated Local File Inclusion in Kelly Young <= 1.1.0 versions.	2026-06-16	8.1	CVE-2025-69141
ThemeREX--Line Agency	Unauthenticated Local File Inclusion in Line Agency <= 1.3.1 versions.	2026-06-17	8.1	CVE-2025-69175
ThemeREX--LuxMed Medicine & Healthcare Doctor WordPress Theme	Unauthenticated Local File Inclusion in LuxMed Medicine & Healthcare Doctor WordPress Theme <= 1.2.2 versions.	2026-06-17	8.1	CVE-2025-69115
ThemeREX--MaxiNet	Unauthenticated Local File Inclusion in MaxiNet <= 1.2.10 versions.	2026-06-16	8.1	CVE-2025-69114
ThemeREX--Medeus	Unauthenticated Local File Inclusion in Medeus <= 1.14 versions.	2026-06-16	8.1	CVE-2025-69150
ThemeREX--Mission	Unauthenticated Local File Inclusion in Mission <= 1.22 versions.	2026-06-16	8.1	CVE-2025-69143
ThemeREX--Modernee	Unauthenticated Local File Inclusion in Modernee <= 1.6.0 versions.	2026-06-16	8.1	CVE-2025-69105
ThemeREX--Neuronet	Unauthenticated Local File Inclusion in Neuronet < 1.14.0 versions.	2026-06-17	8.1	CVE-2025-58952
ThemeREX--Nexio	Unauthenticated Local File Inclusion in Nexio <= 1.10.0 versions.	2026-06-16	8.1	CVE-2025-69113
ThemeREX--Orpheus	Unauthenticated Local File Inclusion in Orpheus <= 1.3 versions.	2026-06-17	8.1	CVE-2025-69171
ThemeREX--Planty	Unauthenticated Local File Inclusion in Planty <= 1.14.0 versions.	2026-06-16	8.1	CVE-2025-69112
ThemeREX--Plumbing	Unauthenticated PHP Object Injection in Plumbing <= 1.6 versions.	2026-06-17	9.8	CVE-2025-69127
ThemeREX--Preservation	Unauthenticated Local File Inclusion in Preservation <= 1.10 versions.	2026-06-17	8.1	CVE-2025-69144
ThemeREX--Printo	Unauthenticated Local File Inclusion in Printo <= 1.11 versions.	2026-06-16	8.1	CVE-2025-69159
ThemeREX--Putter	Unauthenticated Local File Inclusion in Putter <= 1.17 versions.	2026-06-16	8.1	CVE-2025-69147

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ThemeREX--Quirky	Unauthenticated Local File Inclusion in Quirky <= 1.23 versions.	2026-06-17	8.1	CVE-2025-69148
ThemeREX--Raider Spirit	Unauthenticated Local File Inclusion in Raider Spirit <= 1.1.2 versions.	2026-06-16	8.1	CVE-2025-69109
ThemeREX--Reisen	Unauthenticated PHP Object Injection in Reisen <= 1.4.1 versions.	2026-06-17	9.8	CVE-2025-69111
ThemeREX--Resurs	Unauthenticated Local File Inclusion in Resurs <= 1.3 versions.	2026-06-17	8.1	CVE-2025-69172
ThemeREX--Rosaleen	Unauthenticated Local File Inclusion in Rosaleen <= 2.8 versions.	2026-06-16	8.1	CVE-2025-69107
ThemeREX--SeaFood Company	Unauthenticated PHP Object Injection in SeaFood Company <= 1.4 versions.	2026-06-16	9.8	CVE-2025-69122
ThemeREX--Skyward	Unauthenticated Local File Inclusion in Skyward <= 1.10 versions.	2026-06-17	8.1	CVE-2025-69164
ThemeREX--Snow Club	Unauthenticated Local File Inclusion in Snow Club <= 1.1 versions.	2026-06-17	8.1	CVE-2025-69123
ThemeREX--Snowy	Unauthenticated Local File Inclusion in Snowy <= 1.13 versions.	2026-06-17	8.1	CVE-2025-69161
ThemeREX--Spike	Unauthenticated Local File Inclusion in Spike <= 1.2 versions.	2026-06-16	8.1	CVE-2025-69168
ThemeREX--ThemeREX Addons	Unauthenticated PHP Object Injection in ThemeREX Addons <= 2.36.1.1 versions.	2026-06-17	9.8	CVE-2025-60205
ThemeREX--Topsy	Unauthenticated Local File Inclusion in Topsy <= 1.1 versions.	2026-06-17	8.1	CVE-2025-69173
ThemeREX--Top Dog	Unauthenticated Local File Inclusion in Top Dog <= 1.0.5 versions.	2026-06-16	8.1	CVE-2025-69149
ThemeREX--WineShop	Unauthenticated Local File Inclusion in WineShop <= 3.17 versions.	2026-06-16	8.1	CVE-2025-69163
themetechnoun--TrueBooker	Unauthenticated Broken Access Control in TrueBooker <= 1.1.9 versions.	2026-06-15	9.1	CVE-2026-48881
Themeton--Lagom	Deserialization of Untrusted Data vulnerability in Themeton Lagom allows Object Injection. This issue affects Lagom: from n/a through 2.0.	2026-06-17	9.8	CVE-2025-60229
Themeton--The Barber Shop	Deserialization of Untrusted Data vulnerability in Themeton The Barber Shop allows Object Injection. This issue affects The Barber Shop: from n/a through 1.9.	2026-06-17	9.8	CVE-2025-60230
Themeum--Right Way	Unauthenticated Local File Inclusion in Right Way <= 4.0 versions.	2026-06-17	8.1	CVE-2026-22330
Themeum--Skillate	Unauthenticated Cross Site Scripting (XSS) in Skillate <= 1.2.10 versions.	2026-06-17	7.1	CVE-2026-22329
Themeum--Tutor LMS Pro	Unauthenticated SQL Injection in Tutor LMS Pro <= 3.9.6 versions.	2026-06-17	9.3	CVE-2026-22332
Themify--Themify Folo	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themify Folo allows Reflected XSS. This issue affects Themify Folo: from n/a through 1.9.6.	2026-06-17	7.1	CVE-2025-31013
Themovation--Entrepreneur - Booking for Small Businesses WordPress Theme	Subscriber PHP Object Injection in Entrepreneur - Booking for Small Businesses WordPress Theme <= 3.1.3 versions.	2026-06-17	8.8	CVE-2025-69130
Thrive Themes--Thrive Apprentice	Unauthenticated PHP Object Injection in Thrive Apprentice < 10.8.10.2 versions.	2026-06-17	9.8	CVE-2026-49107
tinyhumansai--OpenHuman	The shell tool command allowlist in the SecurityPolicy of OpenHuman desktop agent through 0.54.0 (default Supervised security policy) can be bypassed to execute arbitrary OS commands with the privileges of the	2026-06-17	9.6	CVE-2026-55743

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	desktop user. Two flaws in src/openhuman/security/policy.rs combine: (1) is_args_safe() blocks the find flags -exec and -ok but not the functionally identical -execdir and -okdir, which also execute an arbitrary command for each matched file; and (2) skip_env_assignments() strips leading inline KEY=value environment-variable assignments before allowlist validation, so a command such as GIT_EXTERNAL_DIFF=<cmd> git diff is validated as the allowed git diff but, when executed via the shell, runs <cmd> through git's environment-driven hooks (for example GIT_EXTERNAL_DIFF or GIT_SSH_COMMAND). Because the sandbox is the primary trust boundary between untrusted LLM-processed content and the host operating system, an attacker can achieve remote code execution via indirect prompt injection: a malicious document, email, calendar event, or web page ingested by the agent instructs it to run a benign-looking allowlisted command, resulting in arbitrary command execution, data exfiltration, arbitrary file read/write, and lateral movement on the user's machine. The issue was fixed in commit 60050aa09a870f53ed7e4cd40ed41fd2860329e7 (first released in 0.54.22-staging; first stable release 0.56.0), which blocks -execdir/-okdir for find.			
tinyproxy--tinyproxy	Tinyproxy through 1.11.3, fixed in commit ff45d3b, fails to reconcile conflicting Content-Length and Transfer-Encoding: chunked headers, forwarding both verbatim to the backend while using Content-Length to determine how many request body bytes to consume. Remote attackers can desynchronize the proxy and backend parser state, allowing injection of arbitrary HTTP requests to the backend to enable cache poisoning, access control bypass, and request hijacking.	2026-06-17	9.1	CVE-2026-54387
tinyproxy--tinyproxy	Tinyproxy through 1.11.3, fixed in commit 364cdb6, fails to reject requests containing multiple Content-Length headers with differing values, forwarding all duplicate headers to the backend while using the first value to determine how many request body bytes to consume. Remote attackers can desynchronize the proxy and backend parser state, allowing injection of arbitrary HTTP requests to the backend to enable cache poisoning, access control bypass, and request hijacking.	2026-06-17	9.1	CVE-2026-54388
tinyproxy--tinyproxy	Tinyproxy through 1.11.3, fixed in commit 09312a1, fails to properly validate the Host header during stathost detection, allowing unauthenticated attackers to access the stats page by injecting a matching Host header or bypass detection via port manipulation. Remote attackers can trigger unauthorized access to internal proxy statistics or misroute requests as transparent proxy connections to circumvent access controls.	2026-06-17	8.2	CVE-2026-55202
Tips and Tricks HQ--WP eMember	Unauthenticated SQL Injection in WP eMember < v10.9.4 versions.	2026-06-17	9.3	CVE-2026-54811
TMS--Amelia	Subscriber Privilege Escalation in Amelia <= 2.3 versions.	2026-06-15	8.8	CVE-2026-48889
TMS--Amelia	Unauthenticated Sensitive Data Exposure in Amelia <= 2.2 versions.	2026-06-15	7.5	CVE-2026-40789
TMS--wpDataTables	Unauthenticated SQL Injection in wpDataTables <= 7.3.6 versions.	2026-06-16	9.3	CVE-2026-49080
tnomi--Attendance Manager	Subscriber SQL Injection in Attendance Manager <= 0.6.2 versions.	2026-06-16	7.6	CVE-2026-52712
Tomdever--wpForo Forum	Unauthenticated SQL Injection in wpForo Forum <= 3.0.4 versions.	2026-06-15	9.3	CVE-2026-40798
Tomdever--wpForo Forum	Unauthenticated Broken Authentication in wpForo Forum <= 3.1.0 versions.	2026-06-17	9.8	CVE-2026-49767
Tomdever--wpForo Forum	Unauthenticated PHP Object Injection in wpForo Forum <= 3.1.0 versions.	2026-06-15	9.8	CVE-2026-49769
Tomdever--wpForo Forum	Unauthenticated Broken Access Control in wpForo Forum < 3.0.2 versions.	2026-06-15	7.5	CVE-2026-40767

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
traccar--traccar-client	Traccar Client is a GPS tracking mobile app for sending location updates to private servers using the open-source Traccar platform. In versions 9.7.19 and below, a single crafted deep link can silently hijack all GPS tracking parameters and redirect telemetry to an attacker-controlled server. The app registers a custom org.traccar.client://config deep-link scheme that silently writes attacker-supplied parameters (server URL, device ID, accuracy, distance, and interval) into the app's persistent configuration with no confirmation, notification, or visual indication. A single crafted link delivered via SMS, email, a webpage, or any installed app can therefore reconfigure the app the moment the victim taps it, with no special permissions required. As a result, an attacker can covertly redirect all of the victim's GPS telemetry to their own server at maximum precision and frequency, and the change persists across restarts. This gives the attacker continuous, real-time tracking of the victim's location. This issue has been fixed in version 9.7.20.	2026-06-16	9.3	CVE-2026-48745
truelockmc--streambert	Streambert is a cross-platform Electron Desktop App to stream and download any video media. In versions 2.4.0 and prior, a high-severity Zip Slip vulnerability was identified in Streambert's subtitle extraction logic. The application does not sanitize archive entry filenames during extraction, allowing a malicious archive to perform path traversal and write arbitrary files to the host filesystem. The subtitle extraction process downloads a ZIP archive and extracts its entries. The destination file path is constructed by concatenating the raw archive entry name (extracted.name) directly to the temporary directory path. If a malicious ZIP archive containing directory traversal sequences is processed, it escapes the temporary directory boundaries. The application then writes the extracted payload anywhere on the host filesystem subject to the application's current write permissions. This issue has been fixed in version 2.5.0.	2026-06-16	10	CVE-2026-48055
TURCK--TBEN-LL-SE-M2	Due to the improper neutralization of special elements used in a name parameter a low privileged remote attacker can exploit a command injection vulnerability in the Managed Ethernet Switch, resulting in full system compromise.	2026-06-16	8.8	CVE-2026-5416
tychesoftwares--Order Delivery Date for WooCommerce	Unauthenticated SQL Injection in Order Delivery Date for WooCommerce <= 4.5.1 versions.	2026-06-15	9.3	CVE-2026-42386
Ultimatebeaver--Ultimate Addons for Beaver Builder	WordPress Ultimate Addons for Beaver Builder 1.2.4.1 contains an authentication bypass vulnerability that allows attackers to gain unauthorized access by exploiting the social media login form functionality. Attackers can submit a POST request to the admin-ajax.php endpoint with the uabb-lf-google-submit action, a valid administrator email address, and a valid nonce to obtain session cookies and authenticate as that user.	2026-06-20	9.8	CVE-2019-25763
undici--undici	Impact: The undici WebSocket client enforces maxPayloadSize on the cumulative byte count of fragments in a message but does not enforce a limit on the number of fragments. A malicious WebSocket server can stream many small or empty continuation frames that each pass per-frame and cumulative-size validation, collectively causing unbounded memory growth in the client process. The result is memory exhaustion and a denial of service. Affected applications are those using the undici WebSocket client (new WebSocket(...)) or the WebSocketStream API that can be induced to connect to an attacker-controlled or compromised WebSocket endpoint. All releases starting at undici 6.17.0 are affected. Patches: Upgrade to undici >= 6.26.0, >= 7.28.0, or >= 8.5.0. Workarounds: No workaround is available. The fix must be applied through an upgrade.	2026-06-17	7.5	CVE-2026-12151
undici--undici	Impact: When using Socks5ProxyAgent, undici reuses a single connection pool across different origins without verifying that the pool's origin matches the requested origin. All requests are dispatched through the	2026-06-17	7.5	CVE-2026-6734

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	pool connected to the first origin, regardless of the intended destination. This causes cross-origin request routing: credentials and request data intended for origin B are sent to origin A, responses from the wrong origin are trusted, and HTTPS requests may be silently downgraded to HTTP. Impacted users are applications that use Socks5ProxyAgent (directly or via setGlobalDispatcher) and make requests to more than one origin. This was introduced in undici 7.23.0 via PR #4385 and affects all versions through 8.1.0. Patches: Upgrade to undici v7.26.0 or v8.2.0. Workarounds: Use a separate Socks5ProxyAgent instance per origin, or avoid using Socks5ProxyAgent with multiple origins.			
undici--undici	Impact: The undici WebSocket client enforces maxPayloadSize per-frame but does not enforce the cumulative size of fragmented uncompressed messages. A malicious WebSocket server can stream many small fragments that each pass per-frame validation but collectively exceed the configured limit, causing unbounded memory growth in the client process. The result is memory exhaustion and a denial of service. Affected applications are those using the undici WebSocket client (new WebSocket(...)) that can be induced to connect to an attacker-controlled or compromised WebSocket endpoint. This is a regression specific to undici 8.1.0. The 6.25.0 line shipped the equivalent cumulative check from the start and is unaffected. The 7.x line never had the maxPayloadSize feature and is also unaffected. Patches: Upgrade to undici >= 8.5.0. Workarounds: No workaround is available. The fix must be applied through an upgrade.	2026-06-17	7.5	CVE-2026-9675
undici--undici	Impact: undici's ProxyAgent silently drops the requestTls option when configured with a SOCKS5 proxy URI (socks5:// or socks://). The target HTTPS connection through the SOCKS5 tunnel falls back to Node's default trust store, ignoring user-configured ca, cert, key, rejectUnauthorized, and servername settings. Applications that pin to an internal or corporate CA via requestTls.ca will, when their proxy URI is SOCKS5, get the default Mozilla CA bundle as the trust anchor instead. Any cert signed by any publicly-trusted CA for the target hostname is accepted, breaking the intended pin and enabling MITM read and tamper of the HTTPS exchange. Affected applications are those that use undici's ProxyAgent (or Socks5ProxyAgent directly) with SOCKS5 AND rely on requestTls for TLS scope restriction. The bug was introduced in undici 7.23.0 when SOCKS5 support was added. Patches: Upgrade to undici v7.28.0 or v8.5.0. Workarounds: No workaround is available within the SOCKS5 path. If a SOCKS5 proxy with TLS scope restriction is required and an upgrade is not yet possible, route the traffic through an HTTP-proxy ProxyAgent instead, where requestTls is honored correctly.	2026-06-17	7.4	CVE-2026-9697
Utiliz--Brikk	Subscriber Arbitrary Content Deletion in Brikk <= 3.0.0 versions.	2026-06-16	7.5	CVE-2025-69103
VamTam--Auto Repair	Unauthenticated Cross Site Scripting (XSS) in Auto Repair <= 22.6 versions.	2026-06-17	7.1	CVE-2026-22328
vanyukov--Offload, AI & Optimize with Cloudflare Images	The Offload, AI & Optimize with Cloudflare Images plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.10.2 via the 'account-id' parameter parameter. This is due to insufficient privilege enforcement on the cf_images_do_setup AJAX handler, which requires only the upload_files capability (Author+) rather than manage_options before writing to wp-config.php, combined with the absence of single-quote escaping - sanitize_text_field() does not strip single quotes, and filter_input(INPUT_POST) bypasses wp_magic_quotes() slashing - allowing a single quote in the account-id or api-key parameter to break out of the single-quoted PHP string literal in the write_config() define() statement. This makes it possible for authenticated attackers, with author-level access and above, to execute code on the server. This is possible because the 'cf-images-nonce' nonce required by the AJAX handler is exposed to all Author-level and above users on wp-	2026-06-18	8.8	CVE-2026-9860

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	admin/upload.php via the CFImages JavaScript object, meaning any upload-capable user can satisfy the nonce check and reach the vulnerable wp-config.php write path.			
Vembu--Vembu StoreGrid	Vembu StoreGrid 4.0 contains an unquoted service path vulnerability in the RemoteBackup and RemoteBackup_webServer services that allows local attackers to escalate privileges. Attackers can place a malicious executable in the unquoted path and restart the service to execute code with LocalSystem privileges.	2026-06-19	7.8	CVE-2016-20086
VeronaLabs--Slimstat Analytics	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in VeronaLabs Slimstat Analytics allows Blind SQL Injection. This issue affects Slimstat Analytics: from n/a through 5.4.11.	2026-06-17	8.5	CVE-2026-54818
VideoWhisper.com--Broadcast Live Video	Unauthenticated PHP Object Injection in Broadcast Live Video < 7.1.3 versions.	2026-06-15	9.8	CVE-2026-27053
VideoWhisper.com--Paid Videochat Turnkey Site	Unauthenticated Deserialization of untrusted data in Paid Videochat Turnkey Site <= 7.3.23 versions.	2026-06-15	8.1	CVE-2026-27333
VillaTheme--GIFT4U	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in VillaTheme GIFT4U allows Blind SQL Injection. This issue affects GIFT4U: from n/a through 1.0.10.	2026-06-17	9.3	CVE-2026-54809
vLLM--vLLM	vLLM versions >= 0.10.2 and < 0.13.0 are missing sparse tensor validation in multimodal embeddings processing. Because PyTorch disables sparse tensor invariant checks by default, an attacker can submit crafted embedding requests with malformed (negative or out-of-bounds) tensor indices, when the prompt-embeds feature is enabled, to trigger crashes or resource exhaustion (denial of service), with potential for out-of-bounds/write-what-where memory corruption. This continues CVE-2025-62164, whose prior fix only disabled the feature by default rather than addressing the root cause.	2026-06-20	8.8	CVE-2026-56340
Wasiliy Strecker--Contest Gallery	Unauthenticated SQL Injection in Contest Gallery <= 28.1.6 versions.	2026-06-15	9.3	CVE-2026-40771
WC Lovers--WooCommerce Frontend Manager Ultimate	Subscriber SQL Injection in WooCommerce Frontend Manager - Ultimate < 6.7.7 versions.	2026-06-17	8.5	CVE-2026-22335
WC Product Table--WooCommerce Product Table Lite	Unauthenticated Cross Site Scripting (XSS) in WooCommerce Product Table Lite <= 4.6.3 versions.	2026-06-15	7.1	CVE-2026-34902
WcMultishipping Mondial Relay & Chronopost for Woocommerce--WCMultiShipping	Subscriber SQL Injection in WCMultiShipping <= 3.0.2 versions.	2026-06-15	8.5	CVE-2026-52700
Wdmtech--vAccount	Joomla! Component vAccount 2.0.2 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the vid parameter. Attackers can send GET requests to the vaccount-dashboard/expense endpoint with crafted SQL payloads in the vid parameter to extract sensitive database information including version and database names.	2026-06-19	8.2	CVE-2019-25756
Wdmtech--vBizz	Joomla! Component vBizz 1.0.7 contains an unrestricted file upload vulnerability that allows authenticated attackers to upload arbitrary PHP files by submitting malicious files through the profile_pic parameter. Attackers can upload PHP files via POST requests to the employee view	2026-06-19	8.8	CVE-2019-25758

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	endpoint and execute them from the uploads directory to achieve remote code execution.			
Wdmtech--vBizz	Joomla! Component vBizz 1.0.7 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the paid parameter. Attackers can submit POST requests to the employee management interface with crafted paid array values containing SQL commands to extract sensitive database information including version and database names.	2026-06-19	7.1	CVE-2019-25759
Wdmtech--VMap	Joomla! Component VMap 1.9.6 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code into the latlngbound parameter. Attackers can send GET requests to index.php with the option=com_vmap&task=loadmarker parameters containing SQL injection payloads to manipulate database queries and extract sensitive information.	2026-06-19	8.2	CVE-2019-25753
Wdmtech--vRestaurant	Joomla Component vRestaurant 1.9.4 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the keysearch parameter. Attackers can send POST requests to the menu-listing-layout endpoint with crafted SQL payloads in the keysearch parameter to extract database table names and sensitive information from the database.	2026-06-19	8.2	CVE-2019-25754
Wdmtech--vReview	Joomla Component vReview 1.9.11 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the cmd parameter. Attackers can send POST requests to the editReview task endpoint with URL-encoded SQL UNION statements in the cmd parameter to extract database information including usernames, passwords, and database versions.	2026-06-19	8.2	CVE-2019-25755
Wdmtech--vWishlist	Joomla vWishlist 1.0.1 contains an SQL injection vulnerability that allows authenticated attackers to execute arbitrary SQL queries by injecting malicious code through the vproductid and userid parameters. Attackers can send POST requests to the component with crafted SQL payloads in these parameters to extract sensitive database information including version and database names.	2026-06-19	7.1	CVE-2019-25757
Web Guy--Stop Spammers	Unauthenticated Cross Site Scripting (XSS) in Stop Spammers <= 2026.3 versions.	2026-06-15	7.1	CVE-2026-48876
WebAppick--CTX Feed	Shop manager PHP Object Injection in CTX Feed <= 6.6.26 versions.	2026-06-15	7.2	CVE-2026-39434
WebGeniusLab--Integrio Core	Unauthenticated Local File Inclusion in Integrio Core < 1.2.8 versions.	2026-06-16	8.1	CVE-2026-34894
WebGeniusLab--Softlab Core	Unauthenticated Local File Inclusion in Softlab Core < 1.2.11 versions.	2026-06-16	8.1	CVE-2026-34895
WebGeniusLab--Thegov Core	Unauthenticated Local File Inclusion in Thegov Core < 2.0.23 versions.	2026-06-16	8.1	CVE-2026-34893
Webilia Inc.--Listdom	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Webilia Inc. Listdom allows Blind SQL Injection. This issue affects Listdom: from n/a through 5.4.0.	2026-06-17	9.3	CVE-2026-54819
Webilia Inc.--Listdom	Unauthenticated Privilege Escalation in Listdom <= 5.5.0 versions.	2026-06-15	7.3	CVE-2026-49063
Webkul--Ajax Quiz	Joomla! Component Ajax Quiz 1.8 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the cid parameter. Attackers can send GET requests to index.php with the option=com_ajaxquiz and view=ajaxquiz parameters to extract sensitive database information including table names and column structures.	2026-06-19	8.2	CVE-2017-20262
Webmin--Webmin	The Webmin HTTP server (miniserv.pl) allows unauthenticated attackers to impersonate any user with a configured SSL client certificate by sending a forged HTTP header. A remote attacker can spoof certificate DNs and authenticate as any user. Fixed in 2.641.	2026-06-18	8.1	CVE-2026-56020

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Weborange--Bargain Product VM3	Joomla! Component Bargain Product VM3 1.0 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the product_id parameter. Attackers can supply crafted SQL statements in GET requests to the brainy and alice views to extract sensitive database information.	2026-06-19	8.2	CVE-2017-20261
Weborange--Price Alert	Joomla! Component Price Alert 3.0.2 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the product_id parameter. Attackers can send requests to the subscribeajax view with crafted SQL payloads in the product_id parameter to extract sensitive database information including credentials and configuration data.	2026-06-19	8.2	CVE-2017-20260
websockets--ws	ws is an open source WebSocket client and server for Node.js. All versions from 1.1.0 up to (but not including) 5.2.5, from 6.0.0 up to 6.2.4, from 7.0.0 up to 7.5.11, and from 8.0.0 up to 8.21.0 are affected by a memory exhaustion DoS vulnerability. A peer can send a high volume of exceptionally small fragments and data chunks, with modest network traffic, to force the remote peer into allocating and holding structural wrappers that consume far more memory than the default documented message-size limit, leading to process termination due to OOM. This issue has been fixed in versions 5.2.5, 6.2.4, 7.5.11, and 8.21.0.	2026-06-16	7.5	CVE-2026-48779
WebToffee--WooCommerce PDF Invoices, Packing Slips, Delivery Notes and Shipping Labels	Unauthenticated Sensitive Data Exposure in WooCommerce PDF Invoices, Packing Slips, Delivery Notes and Shipping Labels <= 4.9.4 versions.	2026-06-15	7.5	CVE-2026-49056
Weird-Solutions--TFTP Broadband	TFTP Broadband 4.3.0.1465 contains an unquoted service path vulnerability in the tftpt.exe service binary that allows local attackers to execute arbitrary code with system privileges. Attackers can place a malicious executable in the Program Files directory path that will be executed during service startup or system reboot with LocalSystem privileges.	2026-06-19	7.8	CVE-2020-37250
Winstep--Winstep	Winstep 18.06.0096 contains an unquoted service path vulnerability in the Winstep Xtreme Service that allows local attackers to escalate privileges. Attackers can place malicious executables in the Program Files directory to be executed with LocalSystem privileges when the service starts.	2026-06-19	7.8	CVE-2020-37253
Wise--Wisecleaner	Wise Care 365 4.27 and Wise Disk Cleaner 9.29 contain unquoted service path vulnerabilities in the WiseBootAssistant and SpyHunter 4 Service respectively, allowing local users to execute arbitrary code with SYSTEM privileges. Attackers can insert malicious executables in the system root path that execute during service startup or system reboot with elevated privileges.	2026-06-19	7.8	CVE-2016-20093
WishList Products, LLC.--WishList Member X	Subscriber Arbitrary File Upload in WishList Member X <= 3.29.0 versions.	2026-06-17	9.9	CVE-2026-25446
Wombat Plugins--Advanced Product Fields (Product Addons) for WooCommerce	Shop manager PHP Object Injection in Advanced Product Fields (Product Addons) for WooCommerce <= 1.6.19 versions.	2026-06-15	7.2	CVE-2026-39499
Wondershare--PDFelement	Wondershare PDFelement 5.2.9 contains a privilege escalation vulnerability due to an unquoted service path in the WsAppService Windows service. Local attackers can place a malicious executable in the service path and execute code with LocalSystem privileges upon service restart or system reboot.	2026-06-19	7.8	CVE-2020-37254

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WooCommerce--WooCommerce	WooCommerce 7.1.0 contains a remote code execution vulnerability that allows attackers to execute arbitrary PHP code by injecting shell commands through the product-type parameter. Attackers can send requests to the class-wc-meta-box-product-images.php endpoint with unsanitized product-type values to write malicious PHP files to the web root.	2026-06-20	9.8	CVE-2022-50972
WP Chill--Modula Image Gallery	Author PHP Object Injection in Modula Image Gallery <= 2.14.18 versions.	2026-06-15	7.2	CVE-2026-39481
Wp Directory Kit--WP Directory Kit	Unauthenticated Broken Access Control in WP Directory Kit <= 1.5.0 versions.	2026-06-15	7.5	CVE-2026-39534
WP E-Signature--Signature Add-On for WooCommerce	Unauthenticated Sensitive Data Exposure in Signature Add-On for WooCommerce <= 2.0 versions.	2026-06-15	7.5	CVE-2026-52694
WP Engine--Faust.js	Authentication Bypass Using an Alternate Path or Channel vulnerability in WP Engine Faust.js allows Password Recovery Exploitation. This issue affects Faust.js: from n/a through 1.8.7.	2026-06-15	8.8	CVE-2026-49062
WP Overnight--WooCommerce PDF Invoices & Packing Slips	Shop manager PHP Object Injection in WooCommerce PDF Invoices & Packing Slips < 5.9.0 versions.	2026-06-15	7.2	CVE-2026-39472
WP Swings--Event Tickets Manager for WooCommerce	Unauthenticated Broken Access Control in Event Tickets Manager for WooCommerce <= 1.5.3 versions.	2026-06-15	7.5	CVE-2026-34898
WP Swings--Upsell Order Bump Offer for WooCommerce	Unauthenticated Broken Authentication in Upsell Order Bump Offer for WooCommerce <= 3.1.4 versions.	2026-06-15	7.5	CVE-2026-49110
WP Travel Engine--WP Travel Engine	Unauthenticated PHP Object Injection in WP Travel Engine <= 6.7.12 versions.	2026-06-15	9.8	CVE-2026-49770
WP Travel Engine--WP Travel Engine	Unauthenticated Other Vulnerability Type in WP Travel Engine <= 6.7.10 versions.	2026-06-15	7.5	CVE-2026-49078
WP Travel--WP Travel Gutenberg Blocks	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP Travel WP Travel Gutenberg Blocks allows Blind SQL Injection. This issue affects WP Travel Gutenberg Blocks: from n/a through 3.9.4.	2026-06-17	9.3	CVE-2026-54808
WP User Manager--WP User Manager	Subscriber Arbitrary File Deletion in WP User Manager <= 2.9.16 versions.	2026-06-15	9.9	CVE-2026-49766
wp-buy--SEO Redirection	Unauthenticated Cross Site Scripting (XSS) in SEO Redirection <= 9.17 versions.	2026-06-15	7.1	CVE-2026-52702
wp.insider--Affiliates Manager	Unauthenticated Sensitive Data Exposure in Affiliates Manager <= 2.9.50 versions.	2026-06-15	7.5	CVE-2026-52692
wp.insider--Simple Membership	Unauthenticated Broken Access Control in Simple Membership <= 4.7.1 versions.	2026-06-15	7.5	CVE-2026-34886
WPClever--WPC Product Bundles for WooCommerce	Unauthenticated Broken Access Control in WPC Product Bundles for WooCommerce <= 8.5.3 versions.	2026-06-15	7.5	CVE-2026-48883
WPClever--WPC Product Options	Unauthenticated Arbitrary File Download in WPC Product Options for WooCommerce <= 3.2.1 versions.	2026-06-15	7.5	CVE-2026-49061

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
for WooCommerce				
WPDeveloper--EmbedPress	Unauthenticated Sensitive Data Exposure in EmbedPress <= 4.5.2 versions.	2026-06-15	7.5	CVE-2026-48872
WPExperts--Post SMTP	Unauthenticated Cross Site Scripting (XSS) in Post SMTP <= 3.6.2 versions.	2026-06-15	7.1	CVE-2026-48838
WPFactory--Min Max Step Quantity Limits Manager for WooCommerce	Unauthenticated Cross Site Scripting (XSS) in Min Max Step Quantity Limits Manager for WooCommerce <= 5.2.2 versions.	2026-06-16	7.1	CVE-2026-39437
WPFunnels--WPFunnels Pro	Unauthenticated Cross Site Scripting (XSS) in WPFunnels Pro <= 2.9.4 versions.	2026-06-17	7.1	CVE-2026-49778
WPGraphQL--WPGraphQL	Unauthenticated SQL Injection in WPGraphQL < 2.11.1 versions.	2026-06-15	7.5	CVE-2026-40762
WPLocker--PT Luxa Addons	Subscriber Arbitrary File Upload in PT Luxa Addons <= 1.2.2 versions.	2026-06-17	9.9	CVE-2025-60218
WPManageNinja--Best Payments Plugin for WP	Unauthenticated Bypass Vulnerability in Best Payments Plugin for WP <= 4.6.19 versions.	2026-06-15	7.5	CVE-2026-42655
WPMet--MetForm Pro	Unauthenticated Broken Access Control in MetForm Pro <= 3.9.1 versions.	2026-06-17	9.1	CVE-2026-24611
wpmudev--Branda White Label & Branding, Free Login Page Customizer	The Branda plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.4.29. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it possible for unauthenticated attackers to change arbitrary user's passwords, including administrators, and leverage that to gain access to their account.	2026-06-19	9.8	CVE-2026-11551
WPos--Woocommerce Book Price	Subscriber Arbitrary File Download in Woocommerce Book Price <= 1.3 versions.	2026-06-17	7.5	CVE-2026-22334
WPTasty--AWP Classifieds	Unauthenticated Broken Access Control in AWP Classifieds <= 4.4.4 versions.	2026-06-15	7.5	CVE-2026-39533
Wptimecapsule--Time Capsule Plugin	WordPress Time Capsule Plugin 1.21.16 contains an authentication bypass vulnerability that allows unauthenticated attackers to gain administrative access by sending a crafted POST request with the IWP_JSON_PREFIX header. Attackers can exploit this flaw to obtain valid administrator session cookies and access the WordPress dashboard without providing credentials.	2026-06-20	7.5	CVE-2020-37255
wpWax--Directorist Booking	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in wpWax Directorist Booking allows Blind SQL Injection. This issue affects Directorist Booking: from n/a through 3.0.3.	2026-06-16	8.5	CVE-2026-49073
WPZOOM--WPZOOM Addons for Elementor	Unauthenticated Cross Site Scripting (XSS) in WPZOOM Addons for Elementor <= 1.3.4 versions.	2026-06-17	7.1	CVE-2026-39597
XServer--CloudSecure WP Security	Unauthenticated Broken Authentication in CloudSecure WP Security <= 1.4.7 versions.	2026-06-15	8.1	CVE-2026-42411
xtemos--Hitek	Unauthenticated Local File Inclusion in Hitek < 1.8.3 versions.	2026-06-17	8.1	CVE-2026-39582
Yandex--Punto Switcher	Punto Switcher through 4.5.0.583 contains an unquoted search path element vulnerability that allows local attackers to execute arbitrary code by exploiting the application's call to WinExec without a fully qualified path for RunDll32.exe when invoking shell32.dll Control_RunDLL input.dll. Attackers can place a malicious executable earlier in the search order to achieve arbitrary code execution in the context of the affected user.	2026-06-18	7.8	CVE-2026-25865

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Yannick Lefebvre--Link Library	Contributor Arbitrary File Deletion in Link Library <= 7.8.8 versions.	2026-06-15	7.7	CVE-2026-40779
Yealink--SIP-T46U	A vulnerability was detected in Yealink SIP-T46U 108.87.50.1. The affected element is the function StartReportInformation of the file /api/inner/beforewifitest of the component Web FastCGI Service. The manipulation of the argument port results in stack-based buffer overflow. Access to the local network is required for this attack. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	8	CVE-2026-12218
Yealink--SIP-T46U	A vulnerability has been found in Yealink SIP-T46U 108.86.0.118. This affects the function mod_upgrade.SparePartsUpload of the file /api/upgrade/accupgradebychunk of the component Firmware Chunk Upload handler. Such manipulation of the argument uid leads to stack-based buffer overflow. The attack can only be initiated within the local network. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	8	CVE-2026-12220
Yealink--SIP-T46U	A vulnerability was found in Yealink SIP-T46U 108.86.0.118. This impacts the function sprintf of the file /api/upgrade/upgrade of the component Firmware Chunk Upload Handler. Performing a manipulation of the argument uid/start_offset results in stack-based buffer overflow. The attack needs to be approached within the local network. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	8	CVE-2026-12221
Yealink--SIP-T46U	A vulnerability was determined in Yealink SIP-T46U 108.86.0.118. Affected is the function mod_webd.BlueToothTest of the file /api/inner/bttest of the component Web FastCGI Service. Executing a manipulation of the argument btMac/pin/reserved can lead to stack-based buffer overflow. The attack needs to be done within the local network. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	8	CVE-2026-12222
Yeeaddons--YayMail	Shop manager PHP Object Injection in YayMail <= 4.3.3 versions.	2026-06-15	7.2	CVE-2026-39498
yeoman--environment	Yeoman Environment provides an API to discover, create, and run generators, and to configure where and how a generator is resolved. Versions 2.9.0 through 6.0.0 install missing local generator packages from caller-supplied package names without user confirmation. In downstream consumers that pass attacker-controlled project configuration into this path, this can result in arbitrary package installation and code execution during CLI bootstrap. The vulnerable method is installLocalGenerators(), which calls repository.install() directly without prompting the user. This issue has been fixed in version 6.0.0.	2026-06-16	8.6	CVE-2026-42089
yydevelopment--Advanced 301 and 302 Redirect	Unauthenticated SQL Injection in Advanced 301 and 302 Redirect <= 1.6.9 versions.	2026-06-15	9.3	CVE-2026-49067
Zcontent--Zap Calendar Lite	Joomla! Component Zap Calendar Lite 4.3.4 contains an SQL injection vulnerability that allows unauthenticated attackers to execute arbitrary SQL queries by injecting malicious code through the 'eid' parameter. Attackers can send GET requests to the RSVP plugin endpoint with crafted SQL payloads to extract sensitive database information including database names and table structures.	2026-06-19	8.2	CVE-2017-20268
zephyrproject--zephyr	Zephyr's Bluetooth Classic Hands-Free Profile (HFP) Hands-Free role parser (subsys/bluetooth/host/classic/hfp_hf.c) contains an out-of-bounds write. During Service Level Connection setup the HF sends AT+CIND=? and parses the AG's +CIND: response in cind_handle(), which assigns a per-entry counter index and calls cind_handle_values() for each list element. cind_handle_values() then wrote hf-ind_table[index] = i without verifying that index is within the 20-element int8_t ind_table[] array of struct	2026-06-17	7.1	CVE-2026-10641

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bt_hfp_hf. Because the parser places no cap on the number of +CIND: list entries, a remote Attendant Gateway (a malicious, compromised, or spoofed peer the device connects to over Bluetooth) can send a response with more than 20 recognized indicator entries and drive index arbitrarily large, writing a small attacker-positioned value past the array into adjacent struct fields (feature masks, SDP/version state, the calls[] array, work/atomic bookkeeping) and potentially beyond the static connection pool slot. This yields memory corruption and at least denial of service of the Bluetooth host, triggered by a single malformed AT response with no user interaction. The sibling consumer ag_indicator_handle_values() already performed the equivalent bounds check; this commit adds the same index = ARRAY_SIZE(hf-ind_table) guard to close the gap. Affects builds with CONFIG_BT_HFP_HF enabled; introduced with the original HFP HF CIND parser (~v1.7) and present through v4.4.0.			
Zidithemes--Grip	Subscriber Arbitrary File Upload in Grip <= 1.0.9 versions.	2026-06-17	9.9	CVE-2024-52488
Zozothemes--Restaurt	Subscriber Arbitrary File Upload in Restaurt <= 1.0.4 versions.	2026-06-17	9.9	CVE-2026-22327
Zyxel--GS1900-48HPv2 firmware	A stack-based buffer overflow vulnerability in the CGI program of Zyxel GS1900-48HPv2 firmware versions through 2.90(ABTQ.1)C0 could allow a LAN-based, unauthenticated attacker to exploit the flaw and potentially execute OS commands via a crafted HTTP request.	2026-06-16	8.8	CVE-2026-7273
abhisheksaha11--URL Preview	The URL Preview plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.0 via the 'url' parameter. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.	2026-06-24	7.2	CVE-2026-12100
adegans--AdRotate Banner Manager	The AdRotate Banner Manager plugin for WordPress is vulnerable to PHP Code Injection in all versions up to, and including, 5.17.7 via the 'banner' attribute of the adrotate shortcode. This is due to insufficient input validation and sanitization of the banner shortcode attribute before concatenation into a PHP code string wrapped in W3 Total Cache mfunc or Borlabs Cache fragment markers. This makes it possible for authenticated attackers, with Contributor-level access and above, to execute arbitrary PHP code on the server. This vulnerability requires W3 Total Cache or Borlabs Cache support to be enabled in AdRotate settings.	2026-06-24	8.8	CVE-2026-12242
Adenion--Blog2Social	Unauthenticated Cross Site Scripting (XSS) in Blog2Social <= 8.9.2 versions.	2026-06-26	7.1	CVE-2026-56044
Adobe--Acrobat Reader	Acrobat Reader versions 2020.009.20074, 2020.001.30002, 2017.011.30171, 2015.006.30523 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-23	7.8	CVE-2020-9695
Adrian Tobey--Groundhogg	Sales Representative SQL Injection in Groundhogg <= 4.5 versions.	2026-06-26	8.5	CVE-2026-57667
Ads WPQuads--Ads by WPQuads	Unauthenticated Sensitive Data Exposure in Ads by WPQuads <= 3.0.3 versions.	2026-06-26	7.5	CVE-2026-54824
AF themes--WP Post Author	Contributor SQL Injection in WP Post Author <= 3.9.1 versions.	2026-06-26	8.5	CVE-2026-57643
Ahmad--JS Help Desk	Subscriber Arbitrary File Deletion in JS Help Desk <= 3.1.1 versions.	2026-06-25	7.7	CVE-2026-56054
AKIN Software Computer Import Export Industry and Trade Ltd.--CafePlus	Missing authentication for critical function vulnerability in AKIN Software Computer Import Export Industry and Trade Ltd. CafePlus allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects CafePlus: from 12.05.03 before 12.05.04.	2026-06-23	8.8	CVE-2026-10711

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
akosglys--Syncee Premium Dropshipping & Wholesale	Unauthenticated Broken Access Control in Syncee Premium Dropshipping & Wholesale <= 1.0.27 versions.	2026-06-26	7.5	CVE-2026-54846
Algolplus--Advanced Order Export For WooCommerce	Customer Cross Site Scripting (XSS) in Advanced Order Export For WooCommerce <= 4.0.9 versions.	2026-06-25	7.1	CVE-2026-56042
Amazon Web Services--Language Servers for AWS	Improper trust boundary enforcement in Language Servers for AWS before version 1.65.0 on all supported platforms may allow a for arbitrary code execution. If a local user opens a maliciously crafted workspace, any commands within the project configuration files may be automatically executed. This issue requires the user to trust the workspace when prompted. To remediate this issue, users should upgrade to Language Servers for AWS version 1.65.0 or higher.	2026-06-23	7.8	CVE-2026-12957
Amazon Web Services--Language Servers for AWS	Missing symlink validation in Language Servers for AWS may allow an arbitrary file write outside of the workspace trust boundary. This may occur when a local user opens a workspace with a maliciously crafted symlink that resolves to a file path outside the workspace trust boundary. To remediate this issue, users should upgrade to version 1.69.0 or higher.	2026-06-23	7.8	CVE-2026-12958
Anthropic--Claude Desktop Cowork	Anthropic Claude Desktop Cowork VM image handling (confirmed across v1.1348.0 through v1.2278.0, including v1.1348.0, v1.1617.0, and v1.2278.0) validates only file presence and a version marker string before booting rootfs.img, but does not verify image content integrity at time-of-use. A local attacker with unprivileged code execution as the victim macOS user can modify the VM root filesystem image and have it trusted on subsequent Cowork VM boots, enabling persistent arbitrary code execution in the VM and access to host-mounted directories. The estimated CWE mapping is CWE-353 (Missing Support for Integrity Check).	2026-06-23	8.7	CVE-2026-7574
antlr--ANTLR4	A weakness has been identified in antlr ANTLR4 up to 4.13.2. Affected is an unknown function of the file tool/src/org/antlr/v4/codegen/model/OutputFile.java of the component Grammar Action Block Handler. Executing a manipulation can lead to code injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-28	7.3	CVE-2026-13500
Appsbd--Vitepos	Unauthenticated Sensitive Data Exposure in Vitepos <= 3.4.2 versions.	2026-06-25	7.5	CVE-2026-54841
appsmithorg--appsmith	Appsmith is a platform to build admin panels, internal tools, and dashboards. Prior to 2.1, the bundled Caddy reverse-proxy's admin API - which has no authentication by default - is bound on 0.0.0.0:2019 inside the container. While this listener is not directly published to the host by docker-compose.yml, it is reachable from the Appsmith server process itself or a SSRF vulnerability. An authenticated low-privileged user can therefore drive the SSRF to issue POST /load (or any other admin-API call) against http://0.0.0.0:2019/, fully replacing the live Caddy configuration and taking over the reverse proxy. This vulnerability is fixed in 2.1.	2026-06-24	9.9	CVE-2026-55454
ARforms--ARforms	The ARForms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the `value` parameter of the `arf_save_incomplete_form_data` AJAX action in all versions up to, and including, 7.1.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that will execute whenever an administrator views the "Partial Filled Form Entries" page in the ARForms dashboard.	2026-06-24	7.2	CVE-2026-3652
Autodesk--Fusion	A maliciously crafted webpage, when visited by a user with Autodesk Fusion Desktop running and the MCP extension enabled, can trigger a vulnerability in the MCP extension that could allow arbitrary code execution. A successful exploit may allow code to execute with the privileges of the current user.	2026-06-22	9.6	CVE-2026-10789

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Averta--Master Slider	Unauthenticated Cross Site Scripting (XSS) in Master Slider <= 3.11.2 versions.	2026-06-25	7.1	CVE-2026-56014
Ays Pro--Popup box	Administrator SQL Injection in Popup box <= 6.0.1 versions.	2026-06-26	7.6	CVE-2026-57631
bestwebsoft--Gallery	Contributor SQL Injection in Gallery <= 4.7.8 versions.	2026-06-26	8.5	CVE-2026-57642
bitwarden--server	Bitwarden Server before 2026.5.0 contains a privilege escalation vulnerability that allows authenticated Custom users with ManageUsers permission to remove Admin accounts from an organization by exploiting a missing role hierarchy check in the bulk user-remove endpoint. Attackers can supply Admin organization-user IDs in a bulk DELETE request to bypass the guard enforced on the single-user removal path, effectively removing one or more Admin accounts from an organization.	2026-06-25	7.1	CVE-2026-57520
Bootstrapped Ventures--Visual Link Preview	Subscriber Sensitive Data Exposure in Visual Link Preview <= 2.3.1 versions.	2026-06-25	7.4	CVE-2026-54821
bPlugins--MailChimp Block	Unauthenticated Broken Access Control in MailChimp Block <= 1.1.15 versions.	2026-06-26	8.3	CVE-2026-56063
bPlugins--Panorama Viewer 360 Degree Image + Video Viewer	Contributor Local File Inclusion in Panorama Viewer - 360 Degree Image + Video Viewer <= 1.6.1 versions.	2026-06-26	7.5	CVE-2026-57647
BuddyBoss--Buddyboss Platform	Subscriber PHP Object Injection in Buddyboss Platform <= 3.0.4 versions.	2026-06-26	9.8	CVE-2026-56032
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.39.12, an unauthenticated visitor of any published Budibase app reads every document of the backing MongoDB, CouchDB, Elasticsearch, DynamoDB- PartiQL, or REST-with-JSON-body collection and, where the builder has published a PUBLIC write query, modifies every document of that collection with one HTTP request. enrichContext at packages/server/src/sdk/workspace/queries/queries.ts:121-138 substitutes parameter values into the raw JSON body of a query, then JSON.parses the result. The validator validateQueryInputs at packages/server/src/api/controllers/query/index.ts:61-71 rejects only Handlebars markers ({{, }}) in user input and does not escape JSON metacharacters (" , \, }). A parameter value containing a closing quote and additional keys lifts attacker-controlled fields into the parsed filter object. For Mongo find, the parsed filter passes directly to collection.find() (packages/server/src/integrations/mongodb.ts:506-510). Duplicate-key JSON parsing overrides the builder's {name: "..."} with {name: {\$exists: true}} and returns every document. The same primitive against an updateMany query (mongodb.ts:577-585) widens the filter scope to the full collection while the builder-controlled \$set body runs against every matched document. The authorized middleware at packages/server/src/middleware/authorized.ts:141-148 short-circuits when the query's role is PUBLIC. CSRF is not enforced on this path. POST /api/v2/queries/:queryId (packages/server/src/api/routes/query.ts:63) accepts the call with no session, only an x-budibase-app-id header that is public from the published-app URL. This vulnerability is fixed in 3.39.12.	2026-06-26	10	CVE-2026-54350
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.39.9, `POST /api/pwa/process-zip` at packages/server/src/api/routes/static.ts:24 accepts a builder-uploaded .zip, extracts it with extract-zip@2.0.1 into a temp directory, then for each entry listed in icons.json validates the icon path, opens it, and streams the bytes into MinIO. The resulting object is served back via GET /api/assets/{appId}/pwa/{uuid}.png. extract-zip@2.0.1 preserves absolute symlink targets when restoring symlink entries. The icon-source validator at	2026-06-26	9.6	CVE-2026-54352

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	packages/server/src/api/controllers/static/index.ts:259-268 resolves the icon source string against baseDir (path.resolve), checks resolvedSrc.startsWith(baseDir + path.sep) against that string, and calls fs.existsSync(resolvedSrc) which follows symbolic links to confirm the target exists. None of the three calls reject symbolic-link entries. packages/backend-core/src/objectStore/objectStore.ts:302 then calls (await fsp.open(path)).createReadStream() on the resolved path. fsp.open follows the symlink, the target file's bytes stream into MinIO, and the response of the asset-fetch endpoint returns those bytes verbatim. Result: a workspace-level builder reads any file the server process can open. This vulnerability is fixed in 3.39.9.			
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.39.9, the webhook trigger endpoint in Budibase is publicly accessible and passes the full HTTP request body into automation execution parameters. A mass assignment vulnerability in externalTrigger() allows an attacker to overwrite the internal appld property by including it in the webhook POST body. When the automation is processed asynchronously (the default path for webhooks without a collect step), the worker executes the attacker-defined automation in the context of the victim's workspace, granting full read/write access to the victim's database. This vulnerability is fixed in 3.39.9.	2026-06-26	8.2	CVE-2026-54351
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.39.9, authenticated users with automation permissions can bypass Budibase's SSRF blacklist through DNS rebinding. The outbound fetch flow validates a hostname against the blacklist before the request is sent, but the actual socket connection later performs a separate DNS lookup through node-fetch. Since the validated IPs are never pinned to the connection, an attacker-controlled hostname can return a public IP during validation and a private/internal IP during the real connection. This results in a non-blind SSRF primitive against internal services reachable from the Budibase host, including loopback, RFC1918 ranges, and cloud metadata endpoints. This vulnerability is fixed in 3.39.9.	2026-06-26	8.5	CVE-2026-54353
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.39.0, `GET /api/chat-links/:instance/:token/handoff` is a public endpoint (no auth required) that performs a permanent, state-changing operation: it binds an external chat identity (Slack/Discord/MS Teams) to an authenticated Budibase user account, with no consent UI and no CSRF protection. The session token in the URL is created by the attacker (from their own /link slash command) and embeds the attacker's externalUserId. When an authenticated Budibase victim visits the URL, their account is silently and permanently linked to the attacker's Slack/Discord identity. The server responds with "Authentication succeeded." - no indication of what was linked. This vulnerability is fixed in 3.39.0.	2026-06-26	7.3	CVE-2026-50132
Budibase--budibase	Budibase is an open-source low-code platform. Prior to 3.39.3, the application server exposes an unauthenticated endpoint that generates S3 PutObject presigned URLs using credentials stored in a workspace datasource. The route is protected only by the recaptcha middleware and does not require authentication, table permission, datasource permission, or builder access. A public caller who knows a workspace ID and S3 datasource ID can request a signed upload URL for attacker-controlled bucket and key values. This vulnerability is fixed in 3.39.3.	2026-06-26	7.4	CVE-2026-50136
bytuncay--Kargo Takip	The Kargo Takip plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.2 via the 'api_url' parameter. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. The script echoes internal API response data (specifically the value of any 'auth' key in a JSON response body) verbatim back to the attacker's browser, enabling	2026-06-24	7.2	CVE-2026-12095

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	direct exfiltration of responses from internal services such as cloud instance metadata endpoints.			
Cacti--cacti	Cacti is an open source performance and fault management framework. In versions 1.2.30 and prior, the rfilter request variable was concatenated into a RLIKE SQL clause without sanitization. The endpoint does not require authentication (graph viewing supports guest access via the configured guest user), so the SQLi was reachable pre-auth on installs with guest viewing enabled. This issue was fixed in version 1.2.31.	2026-06-24	9.8	CVE-2026-39893
Cacti--cacti	Cacti is an open source performance and fault management framework. Versions 1.2.30 and prior have unauthenticated LFI through graph_theme and rrdtool IPC serialization hardening. This issue has been resolved in version 1.2.31.	2026-06-24	9.8	CVE-2026-39938
Cacti--cacti	Cacti is an open source performance and fault management framework. Versions 1.2.30 and prior have pre-authentication SQL Injection via unanchored FILTER_VALIDATE_REGEXP in graph_view.php. This issue has been fixed in version 1.2.31.	2026-06-24	9.8	CVE-2026-39955
Cacti--cacti	Cacti is an open source performance and fault management framework. Versions 1.2.30 and prior have a Stored SQL Injection vulnerability through graph_name_regexp in the Reports feature. This issue has been fixed in version 1.2.31.	2026-06-24	7.6	CVE-2026-39951
Cacti--cacti	Cacti is an open source performance and fault management framework. Versions 1.2.30 and prior have SQL Injection through unsanitized unserialize+implode in managers.php. At line 756 of managers.php, the application assigns \$selected_items by calling cacti_unserialize(stripslashes(gnrv('selected_graphs_array'))). The cacti_unserialize() function calls unserialize() with allowed_classes set to false, which prevents object injection but still allows arbitrary string arrays to be deserialized. Then, at lines 760 to 766, the deserialized array values are passed directly into db_execute('DELETE FROM snmpagent_managers WHERE id IN (' . implode(',', \$selected_items) . ')'), where they are imploded into the SQL statement without any integer validation, resulting in SQL Injection when using SNMP agent management permissions. This issue has been fixed in version 1.2.31.	2026-06-25	7.2	CVE-2026-40083
caddyserver--caddy	Caddy is an extensible server platform that uses TLS by default. From 2.7.0 until 2.11.3, the FastCGI transport's splitPos() in modules/caddyhttp/reverseproxy/fastcgi/fastcgi.go misuses golang.org/x/text/search with search.IgnoreCase when the request path contains a non-ASCII byte. Two distinct flaws in that fallback let an attacker mislead Caddy's FastCGI splitting into treating a non-.php (or other configured split_path extension) file as a script. In any deployment where the attacker can place content into a file served via FastCGI (uploads, file storage, etc.), this can be escalated to remote code execution by crafting a URL whose path triggers either flaw. This vulnerability is fixed in 2.11.3.	2026-06-23	8.1	CVE-2026-45135
caddyserver--caddy	Caddy is an extensible server platform that uses TLS by default. Prior to 2.11.4, forward_auth copy_headers deletes the exact client-supplied identity header before copying the trusted value from the auth gateway. But when the request later goes through php_fastcgi, Caddy normalizes HTTP headers into CGI variables by replacing - with _. This lets a client send an underscore alias that survives the forward_auth delete step but becomes the same PHP/FastCGI variable. Result: a remote client can inject or sometimes override identity/group headers trusted by PHP/FastCGI applications behind Caddy. This vulnerability is fixed in 2.11.4.	2026-06-23	8.1	CVE-2026-52845
caddyserver--caddy	Caddy is an extensible server platform that uses TLS by default. Prior to 2.11.4, on Windows, Caddy path matchers treat /private\secret.txt as outside /private/*, but file_server later resolves the same request path as private\secret.txt on disk. An unauthenticated remote client can bypass Caddy path-scoped auth/deny routes protecting /private/*. This vulnerability is fixed in 2.11.4.	2026-06-23	7.5	CVE-2026-52844

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
canboat--canboat	CANBoat through 6.22, fixed in commit a5a22b7, contains an off-by-one global buffer overflow in the searchForPgn() function in analyzer/pgn.c that allows remote attackers to crash the application. Attackers can deliver a crafted NMEA-2000 message with an out-of-range PGN value over CAN bus or N2K-over-IP to trigger an out-of-bounds array access and denial of service.	2026-06-25	7.3	CVE-2026-56790
Canonical--LXD	A privilege escalation vulnerability exists in LXD from 6.0 before 6.9, 5.21.0 before 5.21.5, and 5.0.0 before 5.0.7 regarding the handling of project-restriction policies during snapshot restoration.. An authenticated project operator in a restricted multi-tenant environment can bypass policy restrictions by importing a maliciously crafted instance backup containing restricted configuration keys within a snapshot. When the snapshot is restored, these restricted keys are applied to the live instance without policy validation. Starting the modified instance grants the operator unauthorized host root access.	2026-06-26	7.2	CVE-2026-9640
Canonical--lxd	Broken Access Control in the devLXDInstancePatchHandler component of Canonical LXD allows an untrusted guest to mount, read, and overwrite another guest's custom storage volume via a crafted device PATCH request over /dev/lxd when security.devlxd.management.volumes is enabled.	2026-06-26	8.4	CVE-2026-12411
Cap-go--capgo	Supabase Capgo before 12.128.2 contains an authorization bypass vulnerability in the SECURITY DEFINER record_build_time RPC function that allows unauthenticated attackers to insert arbitrary build-time records. Attackers can exploit this by calling POST /rest/v1/rpc/record_build_time with a public API key to poison billing and quota data for any organization, enabling resource exhaustion and cross-tenant billing manipulation.	2026-06-24	8.2	CVE-2026-56245
Cap-go--capgo	Cap-go capgo (capgo-backend) before 12.128.12 contains an unauthenticated denial-of-service vulnerability arising from the audit_logs table's Row-Level Security (RLS) policy when accessed via the Supabase PostgREST API. Because the PostgreSQL query planner executes costly logic before RLS rejection, unfiltered queries to the public.audit_logs endpoint using the public anon key consistently trigger statement timeouts (PostgREST error 57014). Under concurrency, this exhausts database resources and causes cascading HTTP 500 failures on unrelated endpoints (e.g. /orgs), resulting in an application-layer denial of service.	2026-06-23	7.5	CVE-2026-56248
Cap-go--capgo	Cap-go before 12.128.2 contains a privilege inversion vulnerability in GET /build/logs/:jobId that allows read-only API key holders to cancel running native builds. The endpoint registers an abort listener on the SSE stream that unconditionally invokes cancelBuildOnDisconnect() using the privileged server-side BUILDER_API_KEY when clients disconnect, bypassing the app.build_native permission check required by the explicit POST /build/cancel/:jobId endpoint. Attackers with read-only API keys can repeatedly disrupt native build operations and CI/CD workflows by opening the log stream and dropping the connection.	2026-06-22	7.1	CVE-2026-56280
Capgo--Capgo	Capgo before 12.128.2 contains a broken authentication vulnerability in its API key generation mechanism. API keys are exposed in frontend requests, and the backend fails to validate that keys are securely generated and bound to the authenticated user. An attacker can tamper with the API key parameter in the generation request and supply arbitrary values, generating custom API keys without proper authorization, which can lead to unauthorized access to protected endpoints.	2026-06-24	9.1	CVE-2026-56237
Capgo--Capgo	Capgo before 12.128.2 contains a cross-domain SSO account takeover vulnerability in the provision-user endpoint that allows attackers to merge arbitrary victim accounts based on email match without validating SSO provider domain authorization. An attacker with enterprise org admin access and a malicious IdP can forge SAML assertions containing victim email addresses to trigger account merge and gain full access to victim accounts, organizations, and data.	2026-06-24	8.7	CVE-2026-56223

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Capgo--Capgo	Capgo before 12.128.2 contains an authorization bypass vulnerability in its public API key management handlers (get/put/delete/post). API keys created with mode=all but restricted to a single app via limited_to_apps are only checked for limited_to_orgs and not for limited_to_apps, so an app-scoped key can enumerate, update, and delete sibling API keys belonging to the same account that are outside its declared app scope, enabling tampering with account-level credentials.	2026-06-23	8.3	CVE-2026-56225
Capgo--Capgo	Capgo before 12.128.2 fails to enforce limited_to_orgs and limited_to_apps constraints on subkeys provided via x-limited-key-id header in middlewareKey function. Attackers can bypass subkey scope restrictions by referencing their own subkeys, causing all downstream route handlers to use the unrestricted parent key instead of the scoped subkey.	2026-06-24	8.8	CVE-2026-56232
Capgo--Capgo	Capgo before 12.128.2 contains a security control bypass vulnerability where the PostgREST/RLS plane accepts plaintext API keys through the capgkey header despite enforce_hashed_api_keys being enabled. Attackers can bypass org-level hashed-key enforcement by sending plaintext API keys directly to the PostgREST/RLS plane to access protected resources.	2026-06-23	8.1	CVE-2026-56243
Capgo--Capgo	Capgo before 12.128.2 contains a rate limit bypass vulnerability in the channel_self endpoint that allows attackers to circumvent rate limiting by rotating the user-controlled device_id parameter. Attackers can send multiple requests per second by changing device_id values to flood the channel_devices table and cause database exhaustion.	2026-06-22	8.2	CVE-2026-56324
Capgo--Capgo	Capgo before 12.128.2 contains an authorization bypass vulnerability in POST /private/role_bindings that fails to verify app_id ownership during app-scoped role binding creation. An attacker with administrative privileges in one organization can create role bindings targeting applications owned by other organizations, enabling unauthorized read and modification of victim applications.	2026-06-23	7.2	CVE-2026-56222
Capgo--Capgo	Capgo before 12.128.2 contains a broken object level authorization (BOLA) vulnerability in the POST /build/start/:jobId and POST /build/cancel/:jobId endpoints. The handlers authorize the request based only on the attacker-controlled app_id supplied in the request body and never verify that the jobId in the URL belongs to that app_id (or the same tenant/org) before issuing privileged builder commands with the server-held builder API key. An authenticated user with the app.build_native permission for any app they control can start or cancel arbitrary builder jobs belonging to other tenants by supplying a victim jobId, resulting in cross-tenant build sabotage (denial of service), unauthorized compute actions, and potential billing impact.	2026-06-24	7.6	CVE-2026-56231
Capgo--Capgo	Capgo before 12.128.2 allows non-admin API keys to read webhook signing secrets via Supabase REST due to insufficient row-level security policies on the webhooks table. Attackers can retrieve the webhook secret and forge valid X-Capgo-Signature headers to send authenticated webhook events to configured receivers, breaking webhook authenticity and integrity.	2026-06-24	7.1	CVE-2026-56244
Capgo--Capgo	Capgo before 12.128.2 enforces mandatory two-factor authentication only at the UI level. Sensitive Organization (ORG) management API endpoints (e.g., editing organization details, inviting users) do not validate 2FA completion on the backend. An authenticated Admin user who has not enabled 2FA can replay or modify a previously captured ORG API request to perform privileged organization actions, bypassing the globally enforced 2FA requirement.	2026-06-24	7.1	CVE-2026-56256
Capgo--Capgo	Capgo before 12.128.2 allows direct patching of public.apps.owner_org through PostgREST, bypassing the transfer_app() workflow and creating split-brain ownership. Attackers can directly update apps.owner_org while leaving app_versions.owner_org unchanged, enabling old-org keys to retain access to version data while new-org keys control the app record.	2026-06-24	7.1	CVE-2026-56257

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Capgo--Capgo	Capgo before 12.128.12 fails to filter deleted app versions when joining channels during /updates resolution, allowing deleted bundles to remain selectable. Attackers can continue deploying deleted bundles to devices by exploiting the missing app_versions.deleted filter in channel version joins.	2026-06-22	7.1	CVE-2026-56314
Capgo--Capgo	Capgo before 12.128.2 contains an information disclosure vulnerability in the unauthenticated /updates endpoint that resolves the defaultChannel parameter before enforcing privacy restrictions, allowing attackers to enumerate private channels and leak version/config state. Unauthenticated attackers can probe private channel names and distinguish valid channels from nonexistent ones based on response differences, revealing assigned bundle versions and platform-specific configuration details.	2026-06-23	7.5	CVE-2026-56322
Capgo--Capgo	Capgo before 12.128.2 contains an information disclosure vulnerability in the /functions/v1/channel_self endpoint that allows unauthenticated attackers to enumerate non-public channel names and determine app existence and subscription status. Remote attackers can send GET requests with arbitrary app_id parameters to disclose internal rollout channels, enumerate valid applications across tenants, and leak billing status without authentication or device binding.	2026-06-22	7.5	CVE-2026-56323
cgarvey--Email JavaScript Cloak	The Email JavaScript Cloak plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'email' shortcode in all versions up to, and including, 1.03 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-24	7.2	CVE-2026-10091
Chainlit--chainlit	Chainlit before 2.10.1 contains a session hijacking vulnerability that allows unauthenticated attackers to restore and inherit authenticated user sessions by presenting a valid sessionId during WebSocket session restoration without ownership verification. Attackers can exploit the restore_existing_session path to assume a victim's permissions and roles, enabling unauthorized invocation of tools and access to data restricted to the authenticated victim.	2026-06-22	8.2	CVE-2026-56104
CheckView--CheckView Automated Testing	Unauthenticated Broken Access Control in CheckView Automated Testing <= 2.1.0 versions.	2026-06-25	7.5	CVE-2026-54844
chimurai--http-proxy-middleware	http-proxy-middleware is node.js http-proxy middleware. From 3.0.4 until 3.0.7 and 4.1.1, fixRequestBody() is the library's documented helper for re-emitting a request body that was already consumed by a body parser. When the outgoing Content-Type is multipart/form-data, it rebuilds the body with handlerFormDataBodyData(), which interpolates each req.body key and value directly into the multipart wire format without neutralizing CR/LF. A \r\n inside a value (or key) lets an attacker close the current part and inject an entirely new form part. Because the proxy's own body parser saw a single opaque value, any gateway-side policy or validation performed on req.body is evaluated against a different set of fields than the upstream backend ultimately parses a request/parameter desynchronization across the trust boundary. This vulnerability is fixed in 3.0.7 and 4.1.1.	2026-06-22	7.5	CVE-2026-55603
chrisvrichardson--MapPress Maps for WordPress	Unauthenticated Cross Site Scripting (XSS) in MapPress Maps for WordPress <= 2.97.3 versions.	2026-06-26	7.1	CVE-2026-56011
clearsale--ClearSale Total	The ClearSale Total plugin for WordPress is vulnerable to SQL Injection via the `pagseguro[metodo]` POST parameter of the `clearsale_total_push` AJAX action in all versions up to, and including, 3.4.2. The handler is registered for unauthenticated users (`wp_ajax_nopriv_clearsale_total_push`), and although a `wp_verify_nonce()` check exists, the failing branch's `die()` is commented	2026-06-24	7.5	CVE-2026-8705

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	out so execution continues regardless of nonce validity. On PHP < 8.0 the attacker-supplied `\$metodo` value bypasses the `switch (\$metodo) { case 4: ... }` guard via loose type juggling (the string `4 AND SLEEP(5)` compares equal to integer `4`), reaching an unquoted `UPDATE wp_cs_total_dadosextras SET metodo=\$metodo, ...` query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires the target server to be running PHP < 8.0.			
codemstory--	Unauthenticated SQL Injection in `>œĒ“œĭ”„ë`îŠŕ ê²“î œ ĩ<-ĭ”œĭŽ“~ĭĭ’` <= 5.5.6 versions.	2026-06-26	9.3	CVE-2026-56036
contempoinc-- Real Estate 7	Unauthenticated SQL Injection in Real Estate 7 <= 3.5.9 versions.	2026-06-26	9.3	CVE-2026-54827
corvuspay-- CorvusPay WooCommerce Payment Gateway	Unauthenticated Broken Authentication in CorvusPay WooCommerce Payment Gateway <= 2.7.4 versions.	2026-06-26	7.5	CVE-2026-56029
Cory Marsh-- BitFire Security	Unauthenticated Multiple Vulnerabilities in BitFire Security <= 5.0.3 versions.	2026-06-26	8.6	CVE-2026-56035
Crawl4AI-- Crawl4AI	Crawl4AI before 0.8.8 contains an arbitrary file write vulnerability in the screenshot and PDF endpoints that allows unauthenticated attackers to write files outside the intended directory via symlink and time-of-check-time-of-use (TOCTOU) attacks on the output_path parameter. Remote attackers can exploit insufficient path validation and symlink following to achieve arbitrary file write and potential code execution on systems where the runtime user has write access to executable or cron locations.	2026-06-23	8.1	CVE-2026-56258
Crawl4AI-- Crawl4AI	Crawl4AI before 0.8.7 contains a server-side request forgery vulnerability in the /crawl, /crawl/stream, /md, and /llm endpoints that fetch arbitrary user-supplied URLs without validation. Unauthenticated attackers can bypass the internal-address blocklist using IPv6-mapped IPv4 addresses to reach internal services and cloud metadata endpoints.	2026-06-22	8.6	CVE-2026-56266
Creative Themes--Blocksy Companion Pro	Contributor Remote Code Execution (RCE) in Blocksy Companion Pro <= 2.1.45 versions.	2026-06-26	8.5	CVE-2026-57315
Crocoblock. Jetimpex Inc.-- JetBooking	Unauthenticated SQL Injection in JetBooking <= 4.0.4.1 versions.	2026-06-26	9.3	CVE-2026-54820
Crocoblock. Jetimpex Inc.-- JetEngine	Unauthenticated SQL Injection in JetEngine <= 3.8.10.2 versions.	2026-06-26	9.3	CVE-2026-56068
Crocoblock. Jetimpex Inc.-- JetSmartFilters	Unauthenticated SQL Injection in JetSmartFilters <= 3.8.3 versions.	2026-06-26	9.3	CVE-2026-56067
CusRev-- Customer Reviews for WooCommerce	Unauthenticated Cross Site Scripting (XSS) in Customer Reviews for WooCommerce <= 5.110.1 versions.	2026-06-26	7.1	CVE-2026-56043
Daan.dev--OMGF Pro	Unrestricted Upload of File with Dangerous Type vulnerability in Daan.Dev OMGF Pro allows Using Malicious Files. This issue affects OMGF Pro: from n/a through 5.2.6.	2026-06-25	10	CVE-2026-57700
Daktronics--VFC- DMP-5000	Various versions of Daktronics Controller Firmware could allow authenticated and unauthenticated remote users to escape the intended directory and enumerate arbitrary file system paths.	2026-06-26	9.8	CVE-2026-28701
Daktronics--VFC- DMP-5000	The DMP-5000 devices are shipped with a default administrative web account with weak authentication controls, which are not required to be changed during initial configuration or operation. Using these accounts provides full system access.	2026-06-26	8.1	CVE-2026-31928

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Daktronics--VFC-DMP-5000	The DMP-5000 file service exposes authenticated arbitrary file upload functionality. There are exposed endpoints which allows authenticated users to upload files of any type without validation. No file extension filtering or content inspection is enforced which allows executable binaries and scripts to be accepted and written directly to the server.	2026-06-26	7.1	CVE-2026-33560
danny-avila--LibreChat	LibreChat is an enhanced ChatGPT clone that supports multiple AI providers. Prior to 0.8.5, LibreChat's MCP OAuth implementation does not validate that the resource parameter from OAuth Protected Resource metadata (RFC 9728) matches the configured MCP server URL, allowing a malicious MCP server to steal access tokens intended for a legitimate server. This vulnerability is fixed in 0.8.5.	2026-06-25	8	CVE-2026-54030
danny-avila--LibreChat	LibreChat is an enhanced ChatGPT clone that supports multiple AI providers. Prior to 0.8.4-rc1, LibreChat allows users to configure custom OpenAI-compatible API endpoints by setting a baseURL. This URL is used to construct HTTP requests without any SSRF validation - no private IP check, no scheme restriction, no DNS pinning. An authenticated user can set baseURL to internal network addresses. This vulnerability is fixed in 0.8.4-rc1.	2026-06-25	7.7	CVE-2026-54033
danpros--htmlly	HTMLy CMS through 3.1.1 contains a path traversal vulnerability that allows low-privileged authenticated attackers to relocate arbitrary files by supplying directory traversal sequences in the oldfile parameter at the admin autosave endpoint. Attackers can pass unsanitized traversal sequences directly to file_exists() and rename() functions in admin.php without canonicalization or directory boundary enforcement to cause unintended relocation of any file writable by the web server process to an attacker-specified draft location.	2026-06-25	8.1	CVE-2026-45233
daytonaio--daytona	Daytona is a secure and elastic infrastructure runtime for AI-generated code execution and agent workflows. Prior to 0.184.0, organization invitations could be accepted (and declined) by a user whose email matched the invitation but had not been verified. Daytona authenticates users via OIDC and matches an invitation's target email against the email in the caller's token, but the invitation accept and decline paths did not require that email to be verified, unlike organization creation, which already enforced verification. On identity providers that allow self-service signup and issue a session before the email is verified, an actor could register an address matching a pending invitation, leave it unverified, and accept the invitation, joining the target organization with the role the invitation carried (up to Owner). This vulnerability is fixed in 0.184.0.	2026-06-23	8.4	CVE-2026-54320
daytonaio--daytona	Daytona is a secure and elastic infrastructure runtime for AI-generated code execution and agent workflows. From 0.101.0 until 0.184.0, sandbox previews that were switched from public to private could remain reachable without authentication for a short period after the change, due to a cached visibility state that was not invalidated when the sandbox's visibility changed. This vulnerability is fixed in 0.184.0.	2026-06-23	7	CVE-2026-54321
daytonaio--daytona	Daytona is a secure and elastic infrastructure runtime for AI-generated code execution and agent workflows. Prior to 0.185.0, Daytona's organization role update and delete endpoints authorized the caller as an owner of the organization named in the request path, but resolved and mutated the target role by its identifier alone, without verifying the role belonged to that organization. An authenticated user who owns any organization (organizations are self-service) could therefore modify the permissions of, or delete, a role belonging to a different organization, given that role's identifier. This vulnerability is fixed in 0.185.0.	2026-06-23	7.7	CVE-2026-54322
Dell--Container Storage Modules	Dell Dell Container Storage Modules, version(s) csi-powerstore v2.16.0, csi-unity v2.16.0, csi-powerflex v2.16.0, csi-powermax v2.16.0, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	2026-06-26	8	CVE-2026-40711

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dell--Display and Peripheral Manager	Dell Display and Peripheral Manager (DDPM Windows), versions prior to 2.3, contain an Improper Access Control vulnerability. A low-privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution.	2026-06-25	7.8	CVE-2026-46733
Dell--Display and Peripheral Manager	Dell Display and Peripheral Manager (DDPM Mac), versions prior to 2.3, contain an Improper Certificate Validation vulnerability. A low-privileged attacker with local access could potentially exploit this vulnerability, leading to Protection mechanism bypass.	2026-06-25	7.3	CVE-2026-46734
Dell--Display and Peripheral Manager	Dell Display and Peripheral Manager (DDPM Mac), versions prior to 2.3, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low-privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution.	2026-06-25	7.8	CVE-2026-46735
Dell--Wyse Management Suite	Dell Wyse Management Suite, versions prior to WMS 5.5 HF1, contain an Acceptance of Extraneous Untrusted Data With Trusted Data vulnerability. A low-privileged attacker with remote access could potentially exploit this vulnerability, leading to Remote Code Execution.	2026-06-25	9.8	CVE-2026-41120
Dell--Wyse Management Suite	Dell Wyse Management Suite, versions prior to WMS 5.5 HF1, contain an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Remote Code Execution.	2026-06-25	7.2	CVE-2026-49506
Dell--Wyse Management Suite (WMS)	Dell Wyse Management Suite (WMS), versions prior to WMS 2605, contain an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low-privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	2026-06-22	8.1	CVE-2026-44271
Dell--Wyse Management Suite (WMS)	Dell Wyse Management Suite (WMS), versions prior to WMS 2605, contain an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low-privileged attacker with remote access could potentially exploit this vulnerability, leading to Unauthorized access.	2026-06-22	8.8	CVE-2026-44272
Dell--Wyse Management Suite (WMS)	Dell Wyse Management Suite (WMS), versions prior to WMS 2605, contain an Improper Link Resolution Before File Access vulnerability. A low-privileged attacker with local access could potentially exploit this vulnerability, leading to Unauthorized access.	2026-06-22	7.8	CVE-2026-44274
denoland--deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.7.10, Deno's node:child_process implementation provided an escapeShellArg() helper used when callers passed shell: true to spawn / spawnSync / exec and friends. On Windows, the helper failed to quote arguments that contained cmd.exe metacharacters and did not neutralize % (which cmd.exe expands even inside double-quoted strings). An attacker who controlled any portion of an argument passed to such a call could inject arbitrary additional commands into the spawned cmd.exe invocation. This vulnerability is fixed in 2.7.10.	2026-06-23	8.1	CVE-2026-49402
denoland--deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime. From 2.0.0 until 2.7.8, a flaw in Deno's Node.js tls compatibility layer could cause a TLS client to transmit application data in plaintext after a connection retry. When `autoSelectFamily` was enabled and the first address-family attempt failed, the socket reinitialization path reused a stale TLS upgrade hook that was bound to the original, failed handle. As a result, the replacement TCP connection was never upgraded to TLS, and any data the application wrote before the secureConnect event travelled over the network unencrypted. A network attacker positioned to cause the initial connection attempt to fail (for example, by dropping IPv6 traffic on a dual-stack host) could deterministically trigger the fallback path and observe or tamper with traffic that the application believed was TLS-protected. This vulnerability is fixed in 2.7.8.	2026-06-23	7.4	CVE-2026-44726
denoland--deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.7.14, Deno's permission system enforces filesystem and execution restrictions by comparing the requested path against the path supplied to -	2026-06-23	7.3	CVE-2026-49401

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	-deny-read, --deny-write, --deny-run, or --deny-ffi. On macOS, that comparison was done at the raw-byte level while the APFS filesystem treats different Unicode spellings of the same name as the same file. That means a program could reach a denied path by spelling it differently than the deny rule. This vulnerability is fixed in 2.7.14.			
denoland--deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.8.1, node:crypto.checkPrime(candidate[, options][, callback]) and crypto.checkPrimeSync(candidate[, options]) ran no Miller-Rabin rounds at all when the caller left options.checks at its default of 0. In that mode, the only test applied to the candidate was trial division by the primes up to 17,863. Any composite whose smallest prime factor exceeds that bound - for example the product of two primes just above it, such as 17,881 Ã— 17,891 - was reported as true ("probably prime"). The same divergence affected the lower-level op_node_check_prime / op_node_check_prime_bytes paths that the polyfill calls into. This vulnerability is fixed in 2.8.1.	2026-06-23	7.4	CVE-2026-49440
Design--Stylish Cost Calculator	Unauthenticated Broken Access Control in Stylish Cost Calculator <= 8.3.9 versions.	2026-06-26	7.5	CVE-2026-54847
Dev Kabir--Enable CORS	Unauthenticated Backdoor in Enable CORS <= 2.0.3 versions.	2026-06-26	7.4	CVE-2026-54833
dFactory--Responsive Lightbox	Unauthenticated Cross Site Scripting (XSS) in Responsive Lightbox <= 2.7.6 versions.	2026-06-26	7.1	CVE-2026-56041
Digiwin--EasyFlow .NET	EasyFlow .NET developed by Digiwin has a Session Fixation vulnerability. If unauthenticated remote attackers replace a specific session ID for a user, they can gain the user's privilege once the user logs in.	2026-06-22	7.5	CVE-2026-12581
docling-project--docling	Docling simplifies document processing by parsing diverse formats and providing integrations with the generative AI ecosystem. In versions >= 2.82.0, < 2.91.0, if the HTML backend was explicitly configured for rendering (rendering option by default deactivated), then the Playwright-based rendering feature could allow JavaScript execution and unrestricted network access when processing untrusted HTML documents. An attacker could craft malicious HTML that executes arbitrary JavaScript in the rendering context or makes unauthorized network requests to internal services, potentially leading to SSRF attacks, data exfiltration, or remote code execution in the rendering environment. This vulnerability is fixed in 2.91.0.	2026-06-24	8.2	CVE-2026-44016
docling-project--docling	Docling simplifies document processing by parsing diverse formats and providing integrations with the generative AI ecosystem. Prior to 2.91.0, the EasyOCR model download functionality extracted ZIP archives without validating member paths, enabling Zip Slip attacks. If an attacker could compromise the model download source (via supply chain attack, DNS spoofing, or MITM), they could write arbitrary files to any location writable by the process, potentially achieving remote code execution by overwriting Python files or system binaries, persistent backdoors by modifying startup scripts or SSH keys, and data corruption or system compromise. This vulnerability is fixed in 2.91.0.	2026-06-24	7.5	CVE-2026-44017
docling-project--docling	Docling simplifies document processing by parsing diverse formats and providing integrations with the generative AI ecosystem. From 2.13.0 until 2.74.0, the USPTO patent XML parser used the standard xml.sax.parseString() without protection against XML External Entity (XXE) attacks. An attacker could craft malicious USPTO patent XML files with external entity references that could read arbitrary files from the server filesystem, perform Server-Side Request Forgery (SSRF) attacks, or cause denial of service through entity expansion (Billion Laughs attack). The vulnerability affects three USPTO patent format parsers: ICE (v4.x), Grant v2.5, and Application v1.x. This vulnerability is fixed in 2.74.0.	2026-06-24	7.5	CVE-2026-44020
docling-project--docling	Docling simplifies document processing by parsing diverse formats and providing integrations with the generative AI ecosystem. Prior to 2.94.0,	2026-06-26	7.1	CVE-2026-47214

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the HTML backend has unsafe URI and path handling. This vulnerability is fixed in 2.94.0.			
Dokan Multivendor Plugin--Dokan Pro	Unauthenticated Privilege Escalation in Dokan Pro <= 5.0.4 versions.	2026-06-26	9.8	CVE-2026-56033
dokku--dokku	Dokku is a docker-powered PaaS. Prior to 0.38.2, the git:from-archive and certs:add commands extract user-supplied tar/zip archives into temporary directories without sanitizing member paths or preventing symlink traversal. GNU tar creates symlinks during extraction and follows them for subsequent entries, allowing an attacker to write arbitrary files anywhere writable by the dokku user - including overwriting ~/.ssh/authorized_keys to gain unrestricted shell access. This vulnerability is fixed in 0.38.2.	2026-06-26	9	CVE-2026-45405
dokku--dokku	Dokku is a docker-powered PaaS. Prior to 0.38.2, the openresty-vhosts plugin copies files from an app's openresty/http-includes/ git repository directory to the host and then interpolates their filenames, unescaped, into a single-quoted shell string that is later parsed by eval. A filename containing a single quote breaks the quoting and allows command substitution to execute arbitrary commands on the host as the dokku user during the app's next deploy. This vulnerability is fixed in 0.38.2.	2026-06-26	9	CVE-2026-45406
dokku--dokku	Dokku is a docker-powered PaaS. Prior to 0.38.2, the app name validation regex (^[a-z0-9][^/:_A-Z]*\$) permits shell metacharacters. When an authenticated user pushes to a git remote with a crafted app name, the name is embedded unquoted into a bash pre-receive hook script via an unquoted heredoc (<<EOF instead of <<'EOF') in fn-git-create-hook() at plugins/git/internal-functions:378. On git push, bash interprets the semicolon as a command separator, executing arbitrary commands as the dokku user. This vulnerability is fixed in 0.38.2.	2026-06-26	9	CVE-2026-45408
dokku--dokku	Dokku is a docker-powered PaaS. Prior to 0.38.7, the cron plugin utilizes commands in the app.json file to manage system cron running as the Dokku user. An app.json cron command utilizing special shell characters - including, but not limited to, > or ; - can break out of the Docker container and execute commands on the host as the Dokku user. This vulnerability is fixed in 0.38.7.	2026-06-26	9	CVE-2026-54636
dragonflydb--dragonfly	Dragonfly is an in-memory data store built for modern application workloads. Prior to 1.39.0, a crafted RESTORE payload triggers an out-of-bounds read in DragonflyDB's listpack collection loaders, crashing the entire server process (SIGSEGV). Because DragonflyDB requires no authentication by default and RESTORE is a normal keyspace command, an unauthenticated remote attacker can crash the server with a single ~24-byte command - a remote, repeatable denial of service. This vulnerability is fixed in 1.39.0.	2026-06-26	7.5	CVE-2026-54341
Eagle-Themes--Eagle Booking	Unauthenticated Cross Site Request Forgery (CSRF) in Eagle Booking <= 1.3.4.3 versions.	2026-06-26	8.8	CVE-2025-68052
earendil-works--pi	Pi is a minimal terminal coding harness. From 0.74.0 until 0.78.1, Pi versions with temporary npm or git extension package installs used predictable paths under the operating system temporary directory. On Linux-based multi-user systems, a local attacker who can write to the shared temporary directory could prepare the expected package location before another user runs pi with a temporary extension package source. Pi could then load attacker-controlled extension code in the victim user's process. This vulnerability is fixed in 0.78.1.	2026-06-23	7.3	CVE-2026-54328
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. From 1.37.0 until 1.37.5 and 1.38.3, when the %REQUESTED_SERVER_NAME(X:Y)% is used in log format and host related options is specified, like HOST_FIRST, SNI_FIRST, it's possible to crash Envoy when the specified host header is missing in the request headers. This vulnerability is fixed in 1.37.5 and 1.38.3.	2026-06-26	7.5	CVE-2026-47220

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to 1.35.11, 1.36.7, 1.37.3, and 1.38.1, destructor of JSON Object results in stack overflow when deeply O(100K) nested objects are present. This vulnerability is fixed in 1.35.11, 1.36.7, 1.37.3, and 1.38.1.	2026-06-26	7.5	CVE-2026-48042
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. From 1.23.0 until 1.35.11, 1.36.7, 1.37.3, and 1.38.1, a vulnerability has been identified in Envoy's zstd decompressor implementation (ZstdDecompressorImpl). When zstd decompression is enabled, processing a specially crafted, highly compressed zstd payload can lead to massive memory allocation. An attacker can exploit this to cause severe memory exhaustion, potentially resulting in an Out-Of-Memory (OOM) kill and Denial of Service (DoS) for the Envoy proxy. This vulnerability is fixed in 1.35.11, 1.36.7, 1.37.3, and 1.38.1.	2026-06-26	7.5	CVE-2026-48044
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to 1.35.11, 1.36.7, 1.37.3, and 1.38.1, Envoy can translate a downstream HTTP/3 request that is complete at the transport layer (HEADERS with FIN / headers-only close) but still carries a nonzero Content-Length into a complete upstream HTTP/1 request with unresolved body debt. In an HTTP/1 upstream deployment where the origin replies before reading the declared body and keeps the connection reusable, the beginning of the next Envoy-generated upstream request can be consumed as the first request's body. The remaining bytes are then parsed by the origin as a new HTTP/1 request. This was reproduced as a route-bypass/desync: direct /pwn was denied by Envoy, but the second downstream H3 stream received the response for backend-parsed GET /pwn HTTP/1.1. This vulnerability is fixed in 1.35.11, 1.36.7, 1.37.3, and 1.38.1.	2026-06-26	7.5	CVE-2026-48743
Etoile Web Design Incorporated--Five Star Restaurant Reservations	Unauthenticated Broken Access Control in Five Star Restaurant Reservations <= 2.7.19 versions.	2026-06-25	7.5	CVE-2026-54830
EventPrime--EventPrime	Subscriber PHP Object Injection in EventPrime <= 4.3.4.1 versions.	2026-06-25	8.8	CVE-2026-56053
Everthemess--Goya Core	Contributor Local File Inclusion in Goya Core < 1.0.9.4 versions.	2026-06-26	7.5	CVE-2025-68064
EVoKe--EVoKe CSMS	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to impersonate charging stations. As a result, attackers can exploit this weakness to gain unauthorized access to sensitive data or perform unauthorized actions. Given that no authentication is required, this can lead to privilege escalation and potentially compromise the security of the entire system.	2026-06-25	9.4	CVE-2026-40702
EVoKe--EVoKe CSMS	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence of rate limiting may allow an attacker to conduct denial-of-service attacks or brute-force attacks to gain unauthorized access.	2026-06-25	7.5	CVE-2026-50176
EVoKe--EVoKe CSMS	The WebSocket backend uses charging station identifiers to uniquely associate sessions but allows multiple endpoints to connect using the same session identifier. This implementation results in predictable session identifiers. This vulnerability may allow unauthorized users to authenticate as other users or enable a malicious actor to cause a denial-of-service condition by overwhelming the backend with valid session requests.	2026-06-25	7.3	CVE-2026-54479
expr-eval--expr-eval	All versions of the package expr-eval are vulnerable to Code Execution via the toJSFunction() API. An attacker can execute arbitrary JavaScript by supplying crafted expressions that are compiled into native code using new Function(). Because user-controlled expressions are transformed directly into executable JavaScript, attackers can escape the intended	2026-06-23	9.8	CVE-2026-12866

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	expression sandbox and run arbitrary code within the application's context.			
FasterXML-- jackson-databind	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.10.0 until 2.18.8, 2.21.4, and 3.1.4, jackson-databind's PolymorphicTypeValidator (PTV) is the primary safety mechanism guarding polymorphic deserialization. When polymorphic typing is enabled and a type identifier contains generic parameters (i.e. the type ID string contains <), DatabindContext._resolveAndValidateGeneric() validates only the raw container class name (the substring before <) against the configured PTV. If the container type is approved, the method parses the full canonical type string via TypeFactory.constructFromCanonical() and returns the fully parameterized type without ever validating the nested type arguments against the PTV. The nested type arguments are then resolved, instantiated, and populated as beans during deserialization. An attacker who controls the type ID can therefore place a denied class as a generic type parameter of an allowed container - for example java.util.ArrayList<com.evil.Gadget> when only java.util.ArrayList is allow-listed. The container passes the PTV check; com.evil.Gadget is loaded via Class.forName(name, true, loader), instantiated, and its properties are set from attacker-controlled JSON. This completely bypasses an explicitly configured PTV allow-list. This vulnerability is fixed in 2.18.8, 2.21.4, and 3.1.4.	2026-06-23	8.1	CVE-2026-54512
FasterXML-- jackson-databind	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.10.0 until 2.18.8, 2.21.4, and 3.1.4, BasicPolymorphicTypeValidator.Builder.allowIfSubTypesArray() allowlists any array type based only on clazz.isArray(), without validating the array's component (element) type against the configured allowlist. A PTV built with allowIfSubTypesArray() plus an explicit concrete-type allowlist therefore still permits EvilType[] even though EvilType is not allowlisted. When Jackson deserializes the elements and no per-element type IDs are present, it instantiates the component type directly with no further PTV check, bypassing the allowlist. This vulnerability is fixed in 2.18.8, 2.21.4, and 3.1.4.	2026-06-23	8.1	CVE-2026-54513
feast-dev--feast	Feast before 0.63.0 contains an unsafe deserialization vulnerability that allows unauthenticated or unauthorized attackers to achieve remote code execution by sending a crafted gRPC request to the registry server. The user_defined_function.body field of an OnDemandFeatureView spec is decoded from base64 and passed to dill.loads() before any authorization check is performed, enabling attackers to embed a malicious serialized Python object with an arbitrary __reduce__ method to execute OS commands as the feast service account.	2026-06-24	9.8	CVE-2026-56121
FFmpeg--FFmpeg	FFmpeg's RASC video decoder (decode_dlt in libavcodec/rasc.c) performs 32-bit reads and writes at the row cursor before the NEXT_LINE row-boundary check and validates the DLTA region in pixel rather than byte units, so a DLTA run on a PAL8 frame can access several bytes past the row allocation. A crafted media stream using the RASC FourCC, decoded by libavcodec, triggers a bitstream-controlled out-of-bounds heap write and adjacent out-of-bounds read, leading to memory corruption.	2026-06-28	8.6	CVE-2026-58049
filamentphp-- filament	Filament is a collection of full-stack components for accelerated Laravel development. From 4.0.0 until 4.11.5 and 5.6.5, a flaw in the handling of recovery codes for app-based multi-factor authentication allows the same recovery code to be reused via concurrent submission. This issue does not affect email-based MFA. It also only applies when recovery codes are enabled. If an attacker gains access to both the user's password and their recovery codes, they get two authenticated sessions per recovery code burned instead of one, or more if they batch the parallel submissions wider, materially extending the attacker's window of access compared to	2026-06-22	7.4	CVE-2026-48505

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	what the single-use guarantee implies. This vulnerability is fixed in 4.11.5 and 5.6.5.			
filamentphp-- filament	Filament is a collection of full-stack components for accelerated Laravel development. From 3.0.0 until 3.3.53, a disabled RichEditor field rendered its raw state without sanitizing HTML. Where the data stored in this field's state isn't sanitized already when the form state was filled, an attacker could plant malicious HTML or JavaScript and achieve XSS that executes for users who view the form. This vulnerability is fixed in 3.3.53.	2026-06-22	7.6	CVE-2026-55409
filebrowser-- filebrowser	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Starting with 2.0.0-rc.1, when FileBrowser is configured with proxy authentication (auth.method=proxy), any unauthenticated attacker who can reach the server directly can impersonate any user - including admin - by sending a single forged HTTP header. No credentials are required. Additionally, specifying a non-existent username causes the server to automatically create a new user account, providing an account creation primitive with no authorization. This is an already known issue that has been documented in the documentation for several years, but has not been documented as a vulnerability before.	2026-06-25	9.1	CVE-2026-54089
filebrowser-- filebrowser	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Prior to 2.63.7, `POST /api/share/<path>` accepts an authenticated request for an arbitrary path and stores a public share record without checking whether the target file currently exists. Later, when a file is created at that same path, the previously created public share immediately becomes valid and exposes the new file through `GET /api/public/dl/<hash>`. This vulnerability is fixed in 2.63.7.	2026-06-25	8.4	CVE-2026-54096
filebrowser-- filebrowser	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Prior to 2.63.16, a scoped, non-admin File Browser user holding only the Create permission can delete arbitrary files outside their scope (other tenants' data, and the application's own database) via the upload failure-cleanup path. ScopedFs.RemoveAll is the one dereferencing operation that skips the symlink guard every other method enforces. The direct-upload handler runs RemoveAll on the user-controlled path during failed-upload cleanup, gated only by Perm.Create. If an escaping directory symlink already exists inside the user's scope, an authenticated create-only user can delete an out-of-scope target, bypassing both the ScopedFs boundary and the Perm.Delete gate. This vulnerability is fixed in 2.63.16.	2026-06-25	8.2	CVE-2026-55667
filebrowser-- filebrowser	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Prior to 2.63.6, File Browser's public share handlers rebase the share owner's filesystem root to the shared directory and then evaluate descendant paths against the owner's global and per-user rules using the rebased relative path instead of the original path relative to the owner's scope. As a result, an attacker who knows a public directory share URL can access files and subdirectories that the owner explicitly blocked with rules, as long as those blocked paths are located underneath the shared directory. In the simplest case this is an unauthenticated information disclosure through `GET /api/public/share/*` and `GET /api/public/dl/*`. This vulnerability is fixed in 2.63.6.	2026-06-25	7.5	CVE-2026-54091
filebrowser-- filebrowser	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Prior to 2.63.14, it does not stop the HTTP file handlers from following symbolic links before they open, serve, write, share, or list a file. As a result, a scoped user - and in some cases an unauthenticated public-share recipient - can cross the intended scope boundary by following a symlink whose path is lexically inside their scope but whose target is outside it. This vulnerability is fixed in 2.63.14.	2026-06-25	7.5	CVE-2026-54094

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
FlatPress--FlatPress	FlatPress contains a stored cross-site scripting vulnerability in comment and contact forms where name, URL, and email fields are rendered without proper output encoding in Smarty templates. Attackers can inject arbitrary HTML and JavaScript through these fields to execute malicious scripts in browsers of viewers including administrators, or bypass URL scheme validation to inject javascript: or data: URIs.	2026-06-23	8.2	CVE-2026-56785
Flowise--Flowise	Flowise contains a path traversal vulnerability in the /api/v1/document-store/loader/process endpoint that allows unauthenticated attackers to write arbitrary files to the filesystem. Attackers can exploit unsanitized fileName parameters with ../ sequences to overwrite critical files like package.json and achieve remote code execution when the application restarts.	2026-06-25	10	CVE-2025-71338
Flowise--Flowise	Flowise contains an authentication bypass vulnerability in the unprotected /api/v1/account/register endpoint that allows unauthenticated attackers to create user accounts. Remote attackers can exploit this endpoint to register arbitrary accounts and authenticate to the system, gaining full API access without credentials.	2026-06-25	9.1	CVE-2025-71327
Flowise--Flowise	Flowise before 3.0.6 (affected versions 2.2.8 and earlier) contains an arbitrary file access vulnerability due to missing validation that the chatflowId and chatId parameters are UUIDs or numbers in file handling operations. By supplying a path-traversal value (e.g., '.././.././tmp') as the chatflow id, an unauthenticated attacker can use the /api/v1/chatflows endpoint (via addBase64FilesToStorage) to write arbitrary files, and the /api/v1/get-upload-file and /api/v1/openai-assistants-file/download endpoints (via streamStorageFile) to read arbitrary files. Arbitrary file write may lead to remote code execution.	2026-06-25	9.8	CVE-2025-71334
Flowise--Flowise	Flowise before 3.0.6 (affected versions 2.2.7-patch.1 and earlier) contains an unsandboxed remote code execution vulnerability in the Custom MCP feature, which is designed to execute OS commands such as launching local MCP servers. Because Flowise's authentication and authorization model is minimal and lacks role-based access control, and the default installation runs without authentication unless FLOWISE_USERNAME and FLOWISE_PASSWORD are set, an attacker can send a crafted JSON payload with the header 'x-request-from: internal' to the /api/v1/node-load-method/customMCP endpoint to execute arbitrary OS commands, resulting in complete compromise of the platform container or server.	2026-06-25	9.8	CVE-2025-71336
Flowise--Flowise	Flowise before 3.1.2 contains multiple OS command injection vulnerabilities in the Custom MCP Server feature due to incomplete command-flag validation and a regex bypass in local file access restrictions. An attacker with a Flowise account of any role, or API access with view/update permissions for chatflows, can configure a malicious MCP server to bypass the validateCommandFlags blocklist (for example, 'docker build' is not blocked, and 'npx --yes' is not blocked while only '-y' is) and the validateArgsForLocalFileAccess checks, resulting in execution of arbitrary commands on the Flowise host.	2026-06-23	9.9	CVE-2026-56274
Flowise--Flowise	Flowise before 3.0.10 contains an unverified password change vulnerability. An authenticated user can change their account password through the account settings (Security) section without supplying the current password or any additional verification, as the application does not enforce a current-password check on the credential change. This can lead to full account takeover, particularly if an attacker can hijack or coerce an authenticated session.	2026-06-25	8.3	CVE-2025-71328
Flowise--Flowise	Flowise before 3.0.10 (affected versions 3.0.7 and earlier) fails to invalidate existing sessions and session tokens after a user changes their password. An attacker who already holds an active session, for example via a stolen session token or a device left logged in, remains authenticated as the legitimate user even after the user rotates their credentials, undermining the security purpose of the password change.	2026-06-25	8.1	CVE-2025-71335

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Flowise--Flowise	Flowise before 3.0.10 (affected versions 3.0.7 and earlier) contains an unverified email change vulnerability. An authenticated user can change the account email address, used as a login identifier and password-recovery channel, via the account profile endpoint without confirming the change to the original email address or re-entering the current password. By changing the recovery email, an attacker can take over the account and abuse password reset mechanisms.	2026-06-23	8.3	CVE-2025-71337
Flowise--Flowise	Flowise before 3.0.6 contains an arbitrary file read vulnerability in the chatId parameter of the /api/v1/get-upload-file and /api/v1/openai-assistants-file/download endpoints. The chatId value is not validated and is passed to streamStorageFile(), where a fallback file-lookup path constructed without the orgId is evaluated after the storage-directory containment check, allowing path traversal beyond the intended storage directory. Unauthenticated attackers can read sensitive files such as /root/.flowise/database.sqlite, exposing all database content in the default configuration.	2026-06-25	7.5	CVE-2025-71324
Flowise--Flowise	Flowise before 3.1.2 contains an information disclosure vulnerability in the /api/v1/chatflows/apikey/:apikey endpoint. When the keyonly query parameter is omitted (the default), the endpoint returns not only the chatflows bound to the supplied API key but also all chatflows across every workspace that have no API key assigned, because the underlying query lacks any workspace filter. An attacker with a valid API key for one workspace can therefore retrieve the full ChatFlow configuration (including flowData with system prompts and node configurations, chatbotConfig, apiConfig, and credential IDs) of unprotected chatflows belonging to other workspaces.	2026-06-22	7.7	CVE-2026-56268
Flowise--Flowise	Flowise before 3.1.0 (versions 3.0.13 and earlier) contains a missing authentication vulnerability in the /api/v1/loginmethod endpoint that allows unauthenticated users to retrieve an organization's complete SSO configuration, including OAuth client secrets in cleartext, by providing an organizationId parameter. Remote attackers can send a GET request to harvest sensitive API credentials for Google, Microsoft/Azure, GitHub, and Auth0 integrations. This affects FlowiseAI Cloud and self-hosted instances where the endpoint is exposed.	2026-06-24	7.5	CVE-2026-56270
fpuenteonline--Object Cache 4 everyone	Unauthenticated Sensitive Data Exposure in Object Cache 4 everyone <= 2.3.2 versions.	2026-06-26	7.5	CVE-2026-54834
Frisbii--Frisbii Pay	Contributor Privilege Escalation in Frisbii Pay <= 1.8.2 versions.	2026-06-26	8.8	CVE-2026-56038
FunnelKit--Funnel Builder by FunnelKit	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in FunnelKit Funnel Builder by FunnelKit allows Blind SQL Injection. This issue affects Funnel Builder by FunnelKit: from n/a through 3.15.0.5.	2026-06-24	7.6	CVE-2026-56052
garybowers--bootimus	Bootimus through 0.1.70 contains a broken access control vulnerability that allows authenticated low-privileged users to perform administrative actions by exploiting missing role enforcement in the JWTMiddleware function in internal/auth/auth.go, which validates JWT tokens and account status but fails to inspect the is_admin flag. Attackers can send requests to any endpoint under the /api/users path to create new administrator accounts or reset administrator passwords, thereby gaining full control of the server and the ability to modify boot menus and installation scripts served to PXE clients.	2026-06-23	8.8	CVE-2026-56115
GeoVision Inc.--GV-I/O Box 4E	GV-I/O Box 4E is a smart embedded device with 4 input and 4 relays output that can be controlled over Ethernet and RS-485. DVRSearch is a service running by default on the IOBox listening for UDP messages on port 10001. Any user on the network can send messages to this service and interact with it. Upon receiving a UDP message, the server reads at most 1460 bytes into a local buffer and a pointer to the buffer is stored in a global variable: ##### IP field stack overflow The following code is	2026-06-24	10	CVE-2026-12485

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerable to a stack overflow that is attacker-controlled: v3 = strlen(g_network_config->ip_addr); memcpy(&reply_buf[36], g_network_config->ip_addr, v3);			
GeoVision Inc.-- GV-I/O Box 4E	GV-I/O Box 4E is a smart embedded device with 4 input and 4 relays output that can be controlled over Ethernet and RS-485. DVRSearch is a service running by default on the IOBox listening for UDP messages on port 10001. Any user on the network can send messages to this service and interact with it. Upon receiving a UDP message, the server reads at most 1460 bytes into a local buffer and a pointer to the buffer is stored in a global variable: ##### Net Mask field stack overflow The following code is vulnerable to a stack overflow that is attacker-controlled: v6 = strlen(g_network_config->net_mask); memcpy(&reply_buf[184], g_network_config->net_mask, v6);	2026-06-24	10	CVE-2026-12846
GeoVision Inc.-- GV-I/O Box 4E	GV-I/O Box 4E is a smart embedded device with 4 input and 4 relays output that can be controlled over Ethernet and RS-485. DVRSearch is a service running by default on the IOBox listening for UDP messages on port 10001. Any user on the network can send messages to this service and interact with it. Upon receiving a UDP message, the server reads at most 1460 bytes into a local buffer and a pointer to the buffer is stored in a global variable: ##### Gateway field stack overflow The following code is vulnerable to a stack overflow that is attacker-controlled: v7 = strlen(g_network_config->gateway); memcpy(&reply_buf[216], g_network_config->gateway, v7);	2026-06-24	10	CVE-2026-12847
GeoVision Inc.-- GV-I/O Box 4E	GV-I/O Box 4E is a smart embedded device with 4 input and 4 relays output that can be controlled over Ethernet and RS-485. DVRSearch is a service running by default on the IOBox listening for UDP messages on port 10001. Any user on the network can send messages to this service and interact with it. Upon receiving a UDP message, the server reads at most 1460 bytes into a local buffer and a pointer to the buffer is stored in a global variable: ##### DNS field stack overflow The following code is vulnerable to a stack overflow that is attacker-controlled: v8 = strlen(g_network_config->dns_addr); memcpy(&reply_buf[248], g_network_config->dns_addr, v8);	2026-06-24	10	CVE-2026-12848
GeoVision Inc.-- GV-I/O Box 4E	Multiple OS command injection vulnerabilities exist in the libNetSetObj.so functionality of GeoVision GV-I/O Box 4E 2.09. A specially crafted network packet can lead to command execution. An attacker can send a network request to trigger this vulnerability. `libNetSetObj.so` is an internal library used by various binaries on the device to configure the network stack (start and stop various services, configure IP, Netmask, gateway, dns, etc.) ##### CNetSetObj::m_F_n_Set_IP_Addr command injection The following function takes a string as an ip address, performs no sanitization and calls `system`. This is a classic command injection vulnerability. The function is reachable from both the network-exposed `DVRSearch` service and the `Network.cgi` endpoint. int __fastcall CNetSetObj::m_F_n_Set_IP_Addr(const char **this, char *ip_addr) { bool v2; // zf char v4[72]; // [sp+0h] [bp-48h] BYREF v2 = *this == 0; if (*this) v2 = ip_addr == 0; if (v2) return 0; sprintf(v4, "/sbin/ifconfig %s %s", *this, ip_addr); // attacker controlled ip address system(v4); return 1; }	2026-06-24	9.1	CVE-2026-12486
GeoVision Inc.-- GV-I/O Box 4E	Multiple OS command injection vulnerabilities exist in the libNetSetObj.so functionality of GeoVision GV-I/O Box 4E 2.09. A specially crafted network packet can lead to command execution. An attacker can send a network request to trigger this vulnerability. `libNetSetObj.so` is an internal library used by various binaries on the device to configure the network stack (start and stop various services, configure IP, Netmask, gateway, dns, etc.) ##### CNetSetObj::m_F_n_Set_Net_Mask command injection The following function takes a string as a net mask address, performs no sanitization on it and calls `system`. This is a classic command injection vulnerability. The function is reachable from both the network-exposed `DVRSearch` service and the `Network.cgi` endpoint. int __fastcall	2026-06-24	9.1	CVE-2026-12849

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CNetSetObj::m_F_n_Set_Net_Mask(const char **this, char *netmask_addr) { bool v2; // zf char v4[72]; // [sp+0h] [bp-48h] BYREF v2 = *this == 0; if (*this) v2 = netmask_addr == 0; if (v2) return 0; sprintf(v4, "/sbin/ifconfig %s netmask %s", *this, netmask_addr); // attacker controlled netmask_addr system(v4); return 1; }			
GeoVision Inc.-- GV-I/O Box 4E	Multiple OS command injection vulnerabilities exist in the libNetSetObj.so functionality of GeoVision GV-I/O Box 4E 2.09. A specially crafted network packet can lead to command execution. An attacker can send a network request to trigger this vulnerability. `libNetSetObj.so` is an internal library used by various binaries on the device to configure the network stack (start and stop various services, configure IP, Netmask, gateway, dns, etc.) ##### CNetSetObj::m_F_n_Set_Gate_way command injection The following function takes a string as a gateway address, performs no sanitization on it and calls `system`. This is a classic command injection vulnerability. The function is reachable from both the network-exposed `DVRSearch` service and the `Network.cgi` endpoint. int __fastcall CNetSetObj::m_F_n_Set_Gate_way(const char **this, char *gw, char *dev) { char s[324]; // [sp+4h] [bp-144h] BYREF if (!dev && !*this !gw) return 0; system("/sbin/route del -net 224.0.0.0 netmask 224.0.0.0"); system("/sbin/route del default "); if (dev) sprintf(s, "/sbin/route add default gw %s dev %s", gw, dev); //attacker controlled gw string else sprintf(s, "/sbin/route add default gw %s dev %s", gw, *this); //attacker controlled gw string system(s); sprintf(s, "/sbin/route add -net 224.0.0.0 netmask 224.0.0.0 gw %s dev %s", gw, *this); //attacker controlled gw string system(s); return 1; }	2026-06-24	9.1	CVE-2026-12850
GeoVision Inc.-- GV-I/O Box 4E	Multiple OS command injection vulnerabilities exist in the libNetSetObj.so functionality of GeoVision GV-I/O Box 4E 2.09. A specially crafted network packet can lead to command execution. An attacker can send a network request to trigger this vulnerability. `libNetSetObj.so` is an internal library used by various binaries on the device to configure the network stack (start and stop various services, configure IP, Netmask, gateway, dns, etc.) ##### CNetSetObj::m_F_n_Set_DNS_Addr command injection The following function can take up to two addresses, performs no sanitization and then calls `system`. This is a classic command injection vulnerability. The function is reachable from both the network-exposed `DVRSearch` service and the `Network.cgi` endpoint. int __fastcall CNetSetObj::m_F_n_Set_DNS_Addr(CNetSetObj *this, char *dns1, char *dns2) { int result; // r0 char v5[80]; // [sp+0h] [bp-50h] BYREF if (!dns1) result = 0; if (dns1) { sprintf(v5, "/bin/echo nameserver %s > /etc/resolv.conf", dns1); // attacker controlled dns1 field system(v5); if (dns2) { sprintf(v5, "/bin/echo nameserver %s >> /etc/resolv.conf", dns2); system(v5); } return 1; } return result;	2026-06-24	9.1	CVE-2026-12851
GeoVision Inc.-- GV-LPCLPC2011/2211	An unauthenticated stack-based buffer overflow vulnerability exists in tthttpd in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by insufficient bounds checking when processing web request parameters in a specific request path. A remote attacker may exploit this vulnerability by sending a crafted HTTP request with overly long input, resulting in memory corruption, denial of service, or potentially arbitrary code execution.	2026-06-26	9.8	CVE-2026-57878
GeoVision Inc.-- GV-LPCLPC2011/2211	An unauthenticated stack-based buffer overflow vulnerability exists in ssvr in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by insufficient bounds checking when processing RTSP custom authentication data. A remote attacker may exploit this vulnerability by sending a crafted RTSP request, resulting in memory corruption, denial of service, or potentially arbitrary code execution.	2026-06-26	9.8	CVE-2026-57879
GeoVision Inc.-- GV-LPCLPC2011/2211	An unauthenticated stack-based buffer overflow vulnerability exists in ssvr in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by insufficient bounds checking when parsing RTSP Digest authentication fields. A remote attacker may exploit this	2026-06-26	9.8	CVE-2026-57880

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability by sending a crafted RTSP request containing overly long authentication data, resulting in memory corruption, denial of service, or potentially arbitrary code execution.			
GeoVision Inc.--GV-LPCLPC2011/2211	An unauthenticated stack-based buffer overflow vulnerability exists in vlsvr in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by insufficient length validation when processing remote login data. A remote attacker may exploit this vulnerability by sending crafted login data with overly long input, resulting in memory corruption, denial of service, or potentially arbitrary code execution.	2026-06-26	9.8	CVE-2026-57881
GeoVision Inc.--GV-LPCLPC2011/2211	An unauthenticated format string vulnerability exists in vlsvr in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by improper handling of externally controlled input during log message formatting in the login processing path. A remote attacker may exploit this vulnerability by sending crafted login data, potentially causing information disclosure, memory corruption, or a denial of service.	2026-06-26	8.6	CVE-2026-57877
GeoVision Inc.--GV-LPCLPC2011/2211	An unauthenticated directory traversal vulnerability exists in get_fcont.cgi in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by insufficient validation of user-supplied file path input before the requested file is accessed by the CGI component. A remote attacker may exploit this vulnerability by sending a crafted request to read arbitrary files accessible to the affected process, resulting in information disclosure.	2026-06-26	7.5	CVE-2026-57872
GeoVision Inc.--GV-LPCLPC2011/2211	An unauthenticated NULL pointer dereference vulnerability exists in IEEE8021x_upload.cgi in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by improper validation of multipart upload headers when processing certificate-related upload fields. A remote attacker may exploit this vulnerability by sending a malformed multipart request, causing the affected CGI process to crash and resulting in a denial of service.	2026-06-26	7.5	CVE-2026-57873
GeoVision Inc.--GV-LPCLPC2011/2211	An unauthenticated buffer overflow vulnerability exists in IEEE8021x_upload.cgi in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by insufficient bounds checking when parsing filename values in multipart upload data. A remote attacker may exploit this vulnerability by sending a crafted upload request with overly long input, causing memory corruption and resulting in a denial of service.	2026-06-26	7.5	CVE-2026-57874
GeoVision Inc.--GV-LPCLPC2011/2211	An unauthenticated NULL pointer dereference vulnerability exists in the HTTP request parsing logic of multiple CGI components in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by improper validation of required HTTP request metadata before it is used by the affected components. A remote attacker may exploit this vulnerability by sending a specially crafted HTTP request, causing the affected process to crash and resulting in a denial of service.	2026-06-26	7.5	CVE-2026-57875
GeoVision Inc.--GV-LPCLPC2011/2211	An unauthenticated out-of-bounds write vulnerability exists in onvif.cgi in GeoVision GV-LPC2011 and GV-LPC2211 V1.12 and earlier. The vulnerability is caused by insufficient bounds checking when processing HTTP request body data. A remote attacker may exploit this vulnerability by sending a crafted request with excessive input, causing memory corruption and resulting in a denial of service.	2026-06-26	7.5	CVE-2026-57876
getmaxun--maxun	Maxun before 0.0.42 contains a cross-tenant insecure direct object reference vulnerability in storage and webhook API handlers that allows authenticated users to access other users' robots and OAuth tokens. Attackers can read plaintext Google and Airtable access tokens, modify, delete, or execute other users' robots by bypassing ownership checks in API endpoints.	2026-06-25	8.8	CVE-2026-56767
getsentry--sentry	Sentry is an error tracking and performance monitoring tool. From 24.4.0 until 26.5.2, a Regular Expression Denial of Service (ReDoS) vulnerability exists in Sentry's event ingestion pipeline, where a regex applied to	2026-06-24	7.5	CVE-2026-52794

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker-controlled fields on incoming events can be made to consume disproportionate CPU time. This vulnerability is fixed in 26.5.2.			
Gitea--act_runner	Gitea act_runner with the Docker backend (through act 0.262.0) passes a workflow's container.options string to the Docker job container's HostConfig and, when configured with privileged: false, forces only the Privileged flag off while merging options such as --pid=host, --cap-add, and --security-opt unchanged. A user who can run a workflow on a Docker-backed runner can create a job container with host namespaces and broad capabilities and escape to the host as root despite privileged mode being disabled.	2026-06-28	9.9	CVE-2026-58053
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 16.4 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1 that under certain conditions could have allowed an authenticated user with developer-role permissions to execute arbitrary client-side code in the context of another user's session, due to improper sanitization of user-supplied input.	2026-06-25	8.7	CVE-2026-10086
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.10 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1 that under certain conditions could have allowed an unauthenticated user to execute arbitrary JavaScript in a user's browser session due to improper path validation under certain conditions.	2026-06-25	8	CVE-2026-10712
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 19.1 before 19.1.1 that under certain conditions could have allowed a user to access sensitive information that had already been committed to a project, due to insufficient output filtering in Duo Workflows.	2026-06-25	8.6	CVE-2026-12053
gogs--gogs	Gogs is an open source self-hosted Git service. Prior to 0.14.3, organization names containing path traversal sequences (../) are accepted by Gogs, and repositories under them are written to paths following these path traversals. This allows storing/retrieving data for repositories at arbitrary locations on the filesystem. By creating nested structure of Git repositories, one can overwrite the other's hooks configuration to result in Remote Code Execution (RCE). This vulnerability is fixed in 0.14.3.	2026-06-24	10	CVE-2026-52813
gogs--gogs	Gogs is an open source self-hosted Git service. Prior to 0.14.3, Gogs allows authenticated users to achieve Remote Code Execution (RCE) on the server by creating a pull request with a specially crafted branch name that injects the --exec flag into the git rebase command during the "Rebase before merging" merge operation. This vulnerability is fixed in 0.14.3.	2026-06-24	9.9	CVE-2026-52806
gogs--gogs	Gogs is an open source self-hosted Git service. Prior to 0.14.3, the fix for CVE-2022-1285 prevents adding webhooks or running webhooks with URLs with a hostname that resolves in localCIDRs. However, webhooks still follow redirects allowing to access hostname inside localCIDRs. This vulnerability is fixed in 0.14.3.	2026-06-24	8.3	CVE-2026-47267
gogs--gogs	Gogs is an open source self-hosted Git service. Prior to 0.14.0, as an authorized user, an intruder can dictate the value which is passed to the git diff command which, together with bypassing the filtering of the passed value, allows the user to bypass the target directory and write the result of the comparison to any arbitrary path. This vulnerability is fixed in 0.14.0.	2026-06-24	8.5	CVE-2026-52797
gogs--gogs	Gogs is an open source self-hosted Git service. Prior to 0.14.3, although .ipynb previews are sanitized on the server side via /-/api/sanitize_ipynb, the inserted content is re-rendered on the client side without sanitization using marked() on elements with the .nb-markdown-cell class. During this process, links containing schemes such as javascript: can be regenerated. As a result, when a victim views an attacker-crafted .ipynb file and clicks the link, arbitrary JavaScript is executed in the Gogs origin, leading to a click-based Stored XSS. This vulnerability is fixed in 0.14.3.	2026-06-24	8.9	CVE-2026-52798
gogs--gogs	Gogs is an open source self-hosted Git service. Prior to 0.14.3, organization team member management can be performed via GET requests without CSRF protection. If a victim who is an organization owner is logged in and is tricked into visiting a crafted link, an attacker-controlled user can be added	2026-06-24	8.8	CVE-2026-52800

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to the Owners team. As a result, the attacker gains organization owner-equivalent privileges. This vulnerability is fixed in 0.14.3.			
gogs--gogs	Gogs is an open source self-hosted Git service. Prior to 0.14.3, the Gogs Mirror Settings functionality provide an alternative way from the well protected New Migration functionality for any authenticated users to import local repositories. This issue stems from a lack of validation of SaveAddress function. This vulnerability is fixed in 0.14.3.	2026-06-24	8.1	CVE-2026-52801
gogs--gogs	Gogs is an open source self-hosted Git service. Prior to 0.14.3, a Server-Side Request Forgery (SSRF) vulnerability exists in the repository migration functionality. The application validates only the initially submitted URL hostname, but git clone --mirror follows HTTP redirects. An authenticated user can submit a public URL that redirects to a blocked internal endpoint (e.g., 127.0.0.1), importing the internal repository's contents into an attacker-controlled repository. This vulnerability is fixed in 0.14.3.	2026-06-24	8.7	CVE-2026-52805
gogs--gogs	Gogs is an open source self-hosted Git service. Prior to 0.14.3, GET /attachments/:uuid returns the raw attachment file without verifying whether the requester has view permission for the associated Issue/Comment/Release or the repository. In a test environment with REQUIRE_SIGNIN_VIEW = false, we confirmed that an unauthenticated user can download attachments belonging to a private repository. This vulnerability is fixed in 0.14.3.	2026-06-24	7.5	CVE-2026-52799
gogs--gogs	Gogs is an open source self-hosted Git service. Prior to 0.14.3, three API endpoints - PATCH /api/v1/repos/:owner/:repo/issue-tracker, PATCH /api/v1/repos/:owner/:repo/wiki, and POST /api/v1/repos/:owner/:repo/mirror-sync - are gated by reqRepoWriter() rather than reqRepoAdmin(). The equivalent operations in the web UI sit behind reqRepoAdmin, which requires AccessMode >= AccessModeAdmin. A write-level collaborator (who has AccessMode == AccessModeWrite < AccessModeAdmin) can therefore call these API endpoints directly to disable the native issue tracker or wiki, inject attacker-controlled external tracker/wiki URLs that redirect all repository visitors, or trigger mirror sync - none of which they are authorized to do. This vulnerability is fixed in 0.14.3.	2026-06-24	7.1	CVE-2026-52808
Google--AngularJS	A flaw in AngularJS' Strict Contextual Escaping (SCE) logic allows bypassing certain SCE policies for resource URLs and can lead to arbitrary JavaScript execution within the context of the victim's browser session. SCE's purpose is to ensure that only trusted or safe values are used in certain security-sensitive contexts, such as resource URLs, including URLs that define executable JavaScript scripts, '<iframe>' documents, route templates, etc. A flaw in the logic that tries to match entire URLs against regular expression matchers can result in partial matches for certain types of regular expressions, effectively bypassing the policies and allowing the use of unsafe values as resource URLs. This issue affects AngularJS versions greater than or equal to 1.2.0-rc.3. Note: The AngularJS project was already End-of-Life when this CVE was published and will not receive any updates to address this issue. For more information see the End-of-Life announcement https://docs.angularjs.org/misc/version-support-status .	2026-06-24	7.6	CVE-2026-11998
Grafana--Grafana Enterprise	The public dashboard query endpoint does not limit request body size before processing, allowing unauthenticated attackers to trigger excessive memory allocation by sending arbitrarily large JSON payloads. This can lead to denial of service through memory exhaustion. No valid dashboard access token or authentication is required to exploit this vulnerability.	2026-06-22	7.5	CVE-2026-42127
Grafana--Grafana OSS	The Loki datasource plugin's callResource handler contains a path traversal vulnerability. An authenticated Viewer-role user can escape the plugin's resource sandbox and access administrative Loki endpoints (e.g. /config, /services, /ready) to extract sensitive backend configuration and internal service information.	2026-06-22	7.7	CVE-2026-42129
Grafana--Grafana OSS	The geomap panel's XYZ tile layer has a sanitize-then-interpolate ordering bug. sanitizeTextPanelContent() runs on the raw template string before	2026-06-22	7.3	CVE-2026-9029

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	getTemplateSrv().replace() substitutes the variable value, which uses the glob format with no HTML escaping. The result is passed to OpenLayers via element.innerHTML. An Editor can set a textbox variable's default value to an XSS payload that executes for every user who opens the dashboard. This is a bypass of the CVE-2023-0507 fix			
Grafana--Snowflake Datasource	The Snowflake datasource allows for GET/PUT commands, which can allow any user with access to run queries against the data source to read/write files between the local grafana server and the connected Snowflake host.	2026-06-22	9.6	CVE-2026-28381
H.VIEW--HV-500S6 IP Camera	A vulnerability exists in H.View IP cameras that could allow an authenticated user to supply unsanitized XML fields to the device's certificate generation interface, which are incorporated into a backend certificate creation command without proper input validation. This may allow for command execution with elevated privileges during certificate generation.	2026-06-26	7.2	CVE-2026-55975
H.VIEW--HV-500S6 IP Camera	A vulnerability exists in H.View IP cameras certificate-related upload interfaces allow authenticated users to store arbitrary file content to fixed, persistent filesystem locations without validating file type, structure, or size. This design omission enables the placement of unexpected or malformed data in locations intended for trusted certificate material, which could affect system integrity or behavior even after reboot.	2026-06-26	7.2	CVE-2026-56414
H5P--H5P	Unauthenticated Cross Site Scripting (XSS) in H5P <= 1.17.6 versions.	2026-06-25	7.1	CVE-2026-56006
haiwen--seahub	Seahub before 13.0.23 does not enforce SHARE_LINK_LOGIN_REQUIRED on GET /api/v2.1/share-link-zip-task/, allowing unauthenticated users to bypass authentication. Attackers with a folder share-link token can call the GET endpoint to obtain a filesaver zip token and download entire shared directory trees.	2026-06-25	8.8	CVE-2026-56768
hancock11--WP Forms Connector	The WP Forms Connector plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.8. The plugin registers the REST route wp/v3/user/list/<id> (callback userDetails()) with permission_callback set to '__return_true', and the function's home-grown authentication only verifies that the supplied 'Username' HTTP header maps to an administrator account and that a 'Password' HTTP header is non-empty. It never validates the password with wp_check_password() (unlike the sibling delete_wc_user() function which does). This makes it possible for unauthenticated attackers to retrieve sensitive information for any registered user ID - including the WordPress password hash (user_pass) and email address - by sending a request with a valid administrator login name (commonly the default 'admin') and any arbitrary password value.	2026-06-24	7.5	CVE-2026-9178
hancock11--WP Forms Connector	The WP Forms Connector plugin for WordPress is vulnerable to SQL Injection via the 'order' parameter of the /wp-json/wp/v3/post/list REST endpoint in versions up to and including 1.8. This is due to insufficient escaping on the user-supplied 'order' parameter (read directly from \$_GET['order'] into \$shorting) and the lack of sufficient preparation on the existing SQL query in the listPost() function, where the value is concatenated unquoted into the ORDER BY clause and executed via \$wpdb->get_results() without \$wpdb->prepare(). The endpoint is registered with permission_callback '__return_true' and performs only a broken header-based check that validates the supplied 'Username' corresponds to an administrator account while never verifying the 'Password'. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-06-24	7.5	CVE-2026-9179
hcengineering--platform	Huly Platform through 0.7.423, fixed in commit 68cbf8a contains an authenticated server-side request forgery vulnerability in the /import endpoint of front pod that allows workspace users to make arbitrary server requests. Attackers can exploit this by supplying malicious URLs to	2026-06-25	8.5	CVE-2026-56769

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	fetch internal services, exfiltrate responses, and replay credentials against backend systems.			
HCLSoftware--Traveler for Microsoft Outlook	HCL Traveler for Microsoft Outlook (HTMO) is susceptible to vulnerabilities due to .NET Framework 4.5 being out of service. Since .NET Framework 4.5 has reached end-of-life and no longer receives security updates, it may expose the application to publicly known security weaknesses through vulnerable third-party components.	2026-06-27	7.7	CVE-2023-37524
home-assistant--core	Home Assistant is open source home automation software that puts local control and privacy first. Prior to 2026.6.0, the Konnected integration registers an HTTP endpoint, KonnectedView (homeassistant/components/konnected/__init__.py), that is marked as not requiring authentication (requires_auth = False). A comment next to that line says auth is instead handled "via the access token from configuration." That promise is only half true. Write requests (POST and PUT) are handled by update_sensor(), which does check the request's Authorization: Bearer <token> header against the integration's stored access tokens (using hmac.compare_digest). Read requests (GET) are handled by a separate get() method that has no authentication check at all. This vulnerability is fixed in 2026.6.0.	2026-06-23	7.6	CVE-2026-54317
home-assistant--core	Home Assistant is open source home automation software that puts local control and privacy first. Prior to 2026.5.3, the LocationSensorManager BroadcastReceiver is exported with no permission. Any installed app, with zero runtime permissions, can broadcast a forged Google Play Services LocationResult directly to it; the receiver trusts the extra and forwards it to the user's Home Assistant server as the device's real location. This bypasses Android's developer-mode "Mock Location" gate and allows a local malicious app to drive zone-based automations (unlock door / disarm alarm / open garage) by faking the user's GPS position. This vulnerability is fixed in 2026.5.3.	2026-06-23	7.1	CVE-2026-54318
honojs--hono	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.25, with credentials: true and no explicit origin (the default wildcard), the CORS Middleware reflects the request's Origin and sends Access-Control-Allow-Credentials: true. Any site can then make credentialed cross-origin requests and read the responses, exposing cookie-authenticated endpoints to arbitrary origins. This vulnerability is fixed in 4.12.25.	2026-06-22	7.1	CVE-2026-54290
Hubbell--Aclara Metrum Cellular Web Interface	The Aclara Metrum Cellular Web Interface is vulnerable to unauthorized access due to the absence of authentication controls on critical system functions. This weakness exposes essential configuration settings, allowing attackers to alter operational parameters and trigger system restarts without restriction. Such unauthorized changes can disrupt normal functionality and, if performed repeatedly, may lead to a loss of communications to the device.	2026-06-24	7.5	CVE-2026-1840
IBM--i	IBM WebSphere Application Server and IBM WebSphere Application Server Liberty - when using Intelligent Management with the WebSphere WebServer Plug-in component - are vulnerable to remote code execution and denial of service. This vulnerability can be exploited when an attacker impersonates backend servers and sends crafted responses to the plug-in.	2026-06-22	8.1	CVE-2026-9072
IBM--i	IBM WebSphere Application Server and IBM WebSphere Application Server Liberty are vulnerable to remote code execution and denial of service in the WebSphere Web Server Plug-in component. This vulnerability can be exploited when an attacker impersonates the application server and sends crafted responses to the plug-in.	2026-06-22	7.5	CVE-2026-8858
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.9.3 has an vulnerability due to an improper isolation of Python execution combined with an authentication bypass that allows an unauthenticated attacker to execute arbitrary code on the host system, resulting in complete compromise	2026-06-22	10	CVE-2026-10561
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.8.4 could allow unauthenticated attackers to access protected MCP project resources and execute MCP	2026-06-22	9.8	CVE-2026-7664

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	operations due to improper authorization enforcement in the Streamable MCP transport endpoint.			
IBM--Storage Protect Client	IBM Storage Protect Client 8.1.0.0 through 8.2.1.0 and IBM Storage Protect Snapshot For Windows 8.1.0.0 through 8.2.1.0 could allow a remote attacker to bypass authentication due to the use of a hardcoded credential in the FlashCopy Manager (FCM) authentication mechanism. The application contains a static credential embedded in multiple authentication code paths, and does not properly validate authentication responses, which may allow an unauthenticated attacker to establish a trusted session and access protected services. This vulnerability affects client components across multiple versions and may allow an attacker to impersonate legitimate clients, potentially leading to unauthorized access to system resources.	2026-06-22	9.1	CVE-2026-12628
IBM--WebSphere Application Server	IBM WebSphere Application Server 9.0 and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.6 are vulnerable to HTTP request smuggling. A remote attacker could smuggle a specially crafted request to the application server thereby allowing the attacker to bypass security controls, spoof identity, escalate privilege, and expose sensitive information.	2026-06-22	7.4	CVE-2026-8646
IBM--WebSphere Application Server	IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to server-side request forgery (SSRF) with the Ajax Proxy configured. This may allow an attacker to send unauthorized requests from the system, resulting in a security bypass or information disclosure.	2026-06-22	7.4	CVE-2026-9006
IBM--WebSphere Application Server	IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.6 are vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources.	2026-06-22	7.5	CVE-2026-9071
icc0rz--H5P	Contributor Arbitrary File Deletion in H5P <= 1.17.7 versions.	2026-06-26	7.1	CVE-2026-57321
Igor Benic--Recipe Maker For Your Food Blog from Zip Recipes	Contributor SQL Injection in Recipe Maker For Your Food Blog from Zip Recipes <= 8.2.7 versions.	2026-06-26	8.5	CVE-2026-57663
immich-app--immich	immich is a high performance self-hosted photo and video management solution. From commit 4ffa26c9 until 4eb1003, a reflected cross-site scripting (XSS) vulnerability on the /auth/login page allows an attacker to fully compromise any authenticated user's account with a single link click. The continue query parameter is read from the URL and passed to SvelteKit's redirect() without any scheme or origin validation, allowing attacker-controlled JavaScript to execute inside Immich's origin. The payload then uses the victim's existing session to mint an all-permission API key on their account, leading to persistent account takeover. This vulnerability is fixed in commit 4eb1003.	2026-06-23	9.6	CVE-2026-53662
InspiryThemes--RealHomes	Subscriber PHP Object Injection in RealHomes <= 4.5.3 versions.	2026-06-26	8.8	CVE-2026-56055
Jacob N. Breetvelt--WP Photo Album Plus	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Jacob N. Breetvelt WP Photo Album Plus allows Blind SQL Injection. This issue affects WP Photo Album Plus: from n/a through 9.1.13.005.	2026-06-25	7.5	CVE-2026-54829
Jay Versluis--Child Theme Wizard	Unauthenticated Cross Site Request Forgery (CSRF) in Child Theme Wizard <= 1.4 versions.	2026-06-26	8.2	CVE-2026-57655
jdx--mise	mise manages dev tools like node, python, cmake, and terraform. Prior to 2026.3.10, mise processes .tool-versions files through the Tera template engine during parsing, with the exec() function registered, enabling arbitrary command execution. Unlike .mise.toml files, .tool-versions files are not subject to trust verification in non-paranoid mode. This means an	2026-06-26	9.6	CVE-2026-33646

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker can place a malicious .tool-versions file in a git repository, and when a victim with mise activated cds into the directory, arbitrary commands execute without any trust prompt. This vulnerability is fixed in 2026.3.10.			
jdxx--mise	mise manages dev tools like node, python, cmake, and terraform. Prior to 2026.6.4, mise's trust feature gates config files (mise.toml, .tool-versions) through trust_check, but task-include files are loaded on a path that never reaches it. When a directory has a task-include dir (mise-tasks/, .mise/tasks/,) but no config file, mise falls back to the default includes and renders each task's tera fields - and that tera environment has exec() registered. A {{ exec(command=') }} in any rendered field runs arbitrary commands the moment the tasks are merely listed. There's no config file to gate on, so no trust prompt ever appears. Read-only commands trigger it: mise tasks, mise task ls, mise run, mise tasks --usage (the query shell completion runs on Tab). The victim only has to cd into a cloned repo and list or tab-complete a task. This vulnerability is fixed in 2026.6.4.	2026-06-26	8.6	CVE-2026-55441
Jegstudio--Gutenverse Companion	Unauthenticated Broken Access Control in Gutenverse Companion <= 2.5.0 versions.	2026-06-26	7.5	CVE-2026-54832
jellyfin--jellyfin	Jellyfin is an open source self hosted media server. Prior to 10.11.10, a potential FFmpeg argument injection vulnerability exists in the subtitle conversion code path. SubtitleEncoder.ConvertTextSubtitleToSrtInternal (SubtitleEncoder.cs, line 382) interpolates the subtitle file path into FFmpeg command-line arguments without calling EncodingUtils.NormalizePath(). On Linux, filenames can contain double-quote characters, which break the argument quoting and allow injection of arbitrary FFmpeg arguments. The vulnerability is reachable without authentication via SubtitleController.GetSubtitle, which has no [Authorize] attribute. An attacker who can place a file in a Jellyfin media library directory (shared NAS, Samba share, guest upload) can achieve arbitrary file write on the server and information disclosure. This vulnerability is fixed in 10.11.10.	2026-06-24	8.8	CVE-2026-48793
jellyfin--jellyfin	Jellyfin is an open source self hosted media server. From 10.9.0 until 10.11.10, the POST /ClientLog/Document endpoint accepts the Authorization header's Client and Version fields and uses them unsanitized as components of the on-disk filename when persisting client-uploaded log documents. As a result, any authenticated non-admin user can include ../ sequences in the Client field to cause Jellyfin to write attacker-controlled content to arbitrary paths reachable by the Jellyfin service user, with a forced .log suffix. This vulnerability is fixed in 10.11.10.	2026-06-24	8.8	CVE-2026-49247
Jellywp--NanoMag	Unauthenticated Cross Site Scripting (XSS) in NanoMag <= 1.8 versions.	2026-06-26	7.1	CVE-2026-57325
jetmonsters--Restaurant Menu by MotoPress	Contributor SQL Injection in Restaurant Menu by MotoPress <= 2.4.10 versions.	2026-06-26	8.5	CVE-2026-57644
Johnson & Johnson--Audit Tracking Management System	Johnson & Johnson Audit Tracking Management System (ATMS) before 2026-04-21 allows viewing of meeting minutes and transcripts.	2026-06-26	7.5	CVE-2026-57913
Johnson & Johnson--Campus Recruiting	Johnson & Johnson Campus Recruiting before 2025-10-31 allows viewing of data provided by recruited students, and notes entered about students by interviewers.	2026-06-26	7.5	CVE-2026-57912
joomunited--WP Meta SEO	The WP Meta SEO plugin for WordPress is vulnerable to Unauthenticated Stored Cross-Site Scripting via the REQUEST_URI server variable in all versions up to, and including, 4.5.18. When the plugin's `wpmsTemplateRedirect()` hook detects a 404, it concatenates	2026-06-24	7.2	CVE-2026-9643

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	`\$_SERVER['HTTP_HOST']` with the raw `\$_SERVER['REQUEST_URI']` and inserts that value verbatim into the `wp_wpmc_links.link_url` column via `wpdb->insert()`. This makes it possible for unauthenticated attackers to inject arbitrary web scripts that execute whenever an administrator views the plugin's 404 & Redirects admin page (`/wp-admin/admin.php?page=metaseo_broken_link`).			
jqalang--jq	jq is a command-line JSON processor. Prior to 1.8.2, `jq --rawfile` can turn a handled oversized-string error into invalid-state reuse and a real heap out-of-bounds write in assertion-disabled builds. When `jv_load_file(raw=1)` reads an attacker-controlled file, it repeatedly appends file chunks to the same `jv_string` accumulator. Once `jv_string_append_buf()` returns `jv_invalid_with_msg("String too long")`, the raw-file loop does not stop. If the file contains at least one more byte, the next loop iteration appends a new chunk to an object that is already invalid. With assertions enabled this aborts in `jvp_string_ptr()`. With assertions disabled, the invalid object is interpreted as a string object and ASan reports heap-buffer-overflow. This vulnerability is fixed in 1.8.2.	2026-06-25	7.1	CVE-2026-49839
kestra-io--kestra	Kestra is an open-source, event-driven orchestration platform. Prior to 1.0.45 and 1.3.21, AuthenticationFilter in Kestra OSS uses request.getPath().endsWith("/configs") to whitelist the public configuration endpoint from Basic Auth. Because the check is a suffix match rather than an exact path match, any API path whose last segment is configs bypasses authentication entirely. An unauthenticated remote attacker can exploit this to create and execute arbitrary workflows without credentials. Because Kestra ships with script execution plugins (plugin-script-shell, plugin-script-python, etc.) enabled by default, this directly results in unauthenticated Remote Code Execution as root inside the Kestra worker container. This vulnerability is fixed in 1.0.45 and 1.3.21.	2026-06-26	10	CVE-2026-49869
kestra-io--kestra	Kestra is an open-source, event-driven orchestration platform. Prior to 1.0.45 and 1.3.21, the authentication filter for the REST API (@Filter("/api/v1/*")) treats any request whose path ends in /configs as the public instance-config endpoint and forwards it without a credential check. kestra addresses its resources by URL path segments that the caller chooses (/api/v1/{tenant}/flows/{namespace}, /api/v1/{tenant}/executions/{namespace}/{id}, /api/v1/{tenant}/namespaces/{namespace}/kv/{key}). An anonymous caller picks the literal configs as the final segment, and the request bypasses Basic-Auth entirely. Because the bypass reaches the flow-create and execution-trigger routes, an unauthenticated caller creates a flow containing a Shell or Process task and runs it. The task executes as root inside the kestra container. The official docker-compose.yml mounts /var/run/docker.sock, so root in the container reaches the host Docker daemon. This vulnerability is fixed in 1.0.45 and 1.3.21.	2026-06-26	10	CVE-2026-53576
kestra-io--kestra	Kestra is an open-source, event-driven orchestration platform. Prior to 1.3.24, this vulnerability exists in the BasicAuth authentication component of the Kestra OSS workflow orchestration platform. An attacker who gains read access to the PostgreSQL database can exploit SHA-512's high computation speed to recover the administrator password offline. In Kubernetes deployments, a successful crack further enables reading of the cluster ServiceAccount Token and all K8s Secrets, achieving vertical privilege escalation. This vulnerability is fixed in 1.3.24.	2026-06-26	8.7	CVE-2026-55069
kestra-io--kestra	Kestra is an open-source, event-driven orchestration platform. Prior to 1.0.43 and 1.3.19, several Kestra API endpoints accept a kestra:// URI from the client and pass it through StorageInterface.parentTraversalGuard before reading the underlying file from the local storage backend. The guard only inspects the literal URI.toString(), so a URL-encoded .. written as %2E%2E slips through. The downstream code then calls URI.getPath(), which decodes %2E%2E back to .., and the resulting path is handed to Paths.get(...) without normalization. The OS resolves the .. segments at	2026-06-26	7.7	CVE-2026-45807

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	open(2) time, so an authenticated user with a single execution can read any file the Kestra process has access to on the host filesystem (/etc/passwd, mounted secrets, other tenants' execution outputs, etc.). This vulnerability is fixed in 1.0.43 and 1.3.19.			
kestra-io--kestra	Kestra is an open-source, event-driven orchestration platform. Prior to 1.0.45 and 1.3.23, the local internal-storage backend validates user-supplied paths for .. traversal before it converts Windows-style backslashes to forward slashes. An attacker can therefore smuggle a traversal sequence past the guard using backslashes (..\..\..); the guard sees a harmless string, and the path is only rewritten to ../../../ after validation, immediately before the file is opened. Any authenticated user who can view an execution (the lowest-privilege role) can call GET /api/v1/{tenant}/executions/{executionId}/file?path= and read any file on the server filesystem readable by the Kestra process, outside the storage sandbox and across every tenant and namespace. This includes the embedded H2 database (all flows, all users, all stored secrets), internal storage of every other tenant/namespace, mounted secret files, and the process environment (/proc/self/environ) which contains configured database and secret-backend credentials. It is a complete breach of Kestra's storage isolation and multi-tenancy boundary. This vulnerability is fixed in 1.0.45 and 1.3.23.	2026-06-26	7.7	CVE-2026-49984
kingaddons--Trinity Backup "Backup, Migrate, Restore, Clone & Schedule Backups	Unauthenticated Sensitive Data Exposure in Trinity Backup – Backup, Migrate, Restore, Clone & Schedule Backups <= 2.0.9 versions.	2026-06-26	7.5	CVE-2026-54839
Kludex--python-multipart	Python-Multipart is a streaming multipart parser for Python. Prior to 0.0.30, when parsing application/x-www-form-urlencoded bodies, QuerystringParser located the field separator with a two step lookup: it first scanned the entire remaining buffer for &, and only when no & existed anywhere ahead did it fall back to scanning for ;. For a body that uses ; as the separator and contains no &, every field iteration performed a full failed & scan over the entire remaining buffer before locating the nearby ;. With N semicolon separated fields in a chunk of size B, this yields O(B^2) byte comparisons per chunk. An attacker can submit a small crafted body of the form a;a;a;... and cause the parser to spend seconds of CPU per request. A handful of concurrent requests can exhaust worker processes. This vulnerability is fixed in 0.0.30.	2026-06-22	7.5	CVE-2026-53539
Kludex--starlette	Starlette is a lightweight ASGI framework/toolkit. From 0.4.1 until 1.3.1, request.form() accepts max_fields and max_part_size to bound resource consumption while parsing form data. These limits are enforced for multipart/form-data, but silently ignored for application/x-www-form-urlencoded. An unauthenticated attacker can therefore send a urlencoded body with an arbitrarily large number of fields or an arbitrarily large field, even when the application configured limits it believed would apply. This vulnerability is fixed in 1.3.1.	2026-06-22	7.5	CVE-2026-54283
labstack--echo	Echo is a Go web framework. Prior to 4.15.3 and 5.2.0, Echo's router and static file handler disagree on URL path decoding. The router matches routes using the raw encoded path (preserving %2F as-is), while StaticDirectoryHandler unescapes %2F to / before resolving filesystem paths. This allows an attacker to bypass route-level access controls and read static files without authorization. This vulnerability is fixed in 4.15.3 and 5.2.0.	2026-06-26	7.5	CVE-2026-55677
langflow-ai--langflow	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.2, the "Shareable Playground" (or "Public Flows" in code) contains a critical RCE vulnerability. Shareable Playground feature works by enabling the execution of workflows by unauthenticated users, by accessing a link. Specifically, it enables the route	2026-06-23	9.6	CVE-2026-48519

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	/api/v1/build_public_tmp to execute any public flow, given a public flow ID. When the route executes the flow, it allows for providing arbitrary custom Python code as the nodes code, inside the JSON payload. The vulnerable field is data.nodes[X].data.node.template.code.value. This vulnerability is fixed in 1.9.2.			
langflow-ai--langflow	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.2, an Insecure Direct Object Reference (IDOR) vulnerability in /api/v1/responses endpoint allows an authenticated attacker to execute any flow belonging to another user by specifying the victim's flow ID in the request. This vulnerability is fixed in 1.9.2.	2026-06-23	9.9	CVE-2026-55255
langflow-ai--langflow	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.2, by controlling a files that are digested into the RAG, an attacker can direct the node to read any file on the file-system by absolute path. All components based on BaseFileComponent are vulnerable to the vulnerability. This includes Docling (DoclingInlineComponent), Docling Serve, DoclingRemoteComponent), Read File (FileComponent), NVIDIA Retriever Extraction (NvidiaIngestComponent), Video File (VideoFileComponent), and Unstructured API (UnstructuredComponent). This vulnerability is fixed in 1.9.2.	2026-06-23	9.6	CVE-2026-55447
langflow-ai--langflow	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.1, unauthenticated users can upload any amount of data to the server without any limitations. No need for any prior knowledge, only network access to Langflow. This can lead to space exhaustion on the server. In addition, in the response, the absolute path of the uploaded file is reported to the attacker, which is an information leak that can assist in chaining other primitives. This vulnerability is fixed in 1.9.1.	2026-06-23	9.3	CVE-2026-55450
langflow-ai--langflow	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.0, Langflow's /api/v1/monitor router exposes 7 endpoints that perform read, write, and delete operations on user-owned resources - messages, sessions, build artifacts, and LLM transaction logs - without verifying that the authenticated requester owns the targeted resource. Any authenticated user can read, modify, rename, or permanently delete another user's data by supplying the target's resource ID or flow_id. This is a classic IDOR/BOLA vulnerability. Notably, the same source file (monitor.py) contains one correctly-implemented endpoint that uses an ownership check, demonstrating the correct pattern was known but inconsistently applied. This vulnerability is fixed in 1.9.0.	2026-06-23	8.8	CVE-2026-33760
langflow-ai--langflow	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.0.19, an attacker can send a /api/v1/files/upload/ request without any authentication token/cookies and abuse a very long multipart form boundary to make the langflow app unusable for all users for an indefinite amount of time. This vulnerability is fixed in 1.0.19.	2026-06-23	7.5	CVE-2026-55446
libssh2--libssh2	libssh2 through 1.11.1 reads an attacker-controlled 32-bit attribute count from a publickey-subsystem response and uses it in the allocation num_attrs * sizeof(libssh2_publickey_attribute) without bounds checking, so on 32-bit platforms the multiplication overflows to an undersized buffer. A malicious SSH server can then drive the attribute-parsing loop to write past the allocation, causing a heap buffer overflow in a connecting libssh2 client.	2026-06-28	7	CVE-2026-58050
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: fix fragment reassembly length accounting batman-adv keeps a running payload length for queued fragments and uses it to validate a fragment chain before reassembly. That accounting currently allows the accumulated fragment length to be truncated during updates. As a result, malformed fragment chains can bypass the intended validation and drive reassembly with inconsistent length state, leading to a local denial of service. Fix the accounting by storing the accumulated length in a length-	2026-06-24	9.8	CVE-2026-52914

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	typed field and rejecting update overflows before the existing validation logic runs. The fix was verified against the original reproducer and against valid fragment reassembly paths.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: purge outqueue on stale COOKIE-ECHO handling sctp_stream_update() is only invoked when the association is moved into COOKIE_WAIT during association setup/reconfiguration. In this path, the outbound stream scheduler state (stream->out_curr) is expected to be clean, since no user data should have been transmitted yet unless the state machine has already partially progressed. However, a corner case exists in sctp_sf_do_5_2_6_stale(): when a Stale Cookie ERROR is received, the association is rolled back from COOKIE_ECHOED to COOKIE_WAIT. In this scenario, user data may already have been queued and even bundled with the COOKIE-ECHO chunk. During the rollback, sctp_stream_update() frees the old stream table and installs a new one, but it does not invalidate stream->out_curr. As a result, out_curr may still point to a freed sctp_stream_out entry from the previous stream state. Later, SCTP scheduler dequeue paths (FCFS, RR, PRIO, etc.) rely on stream->out_curr->ext, which can lead to use-after-free once the old stream state has been released via sctp_stream_free(). This results in crashes such as (reported by Yuqi): BUG: KASAN: slab-use-after-free in sctp_sched_fcfs_dequeue+0x13a/0x140 Read of size 8 at addr ff1100004d4d3208 by task mini_poc/9312 CPU: 1 UID: 1001 PID: 9312 Comm: mini_poc Not tainted 7.1.0-rc1-00305-gbd3a4795d574 #5 PREEMPT(full) sctp_sched_fcfs_dequeue+0x13a/0x140 sctp_outq_flush+0x1603/0x33e0 sctp_do_sm+0x31c9/0x5d30 sctp_assoc_bh_rcv+0x392/0x6f0 sctp_inq_push+0x1db/0x270 sctp_rcv+0x138d/0x3c10 Fix this by fully purging the association outqueue when handling the Stale Cookie case. This ensures all pending transmit and retransmit state is dropped, and any scheduler cached pointers are invalidated, making it safe to rebuild stream state during COOKIE_WAIT restart. Updating only stream->out_curr would be insufficient, since queued and retransmittable data would still reference the old stream state and trigger later use-after-free in dequeue paths.	2026-06-24	9.8	CVE-2026-52924
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: tp_meter: avoid use of uninit sender vars batadv_tp_rcv_ack() and batadv_tp_stop() are only valid for tp_vars in the BATADV_TP_SENDER role. When called with a BATADV_TP_RECEIVER role, it proceeds to read sender-only members that were never initialized, leading to undefined behavior. This can be triggered when a node that is currently acting as a receiver in an ongoing tp_meter session receives a malicious ACK packet. Guard against this by checking tp_vars->role immediately after the lookup and bailing out if it is not BATADV_TP_SENDER, before any of those members are accessed.	2026-06-24	9.8	CVE-2026-52931
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: Fix potential out-of-bounds access in crush_decode() A message of type CEPH_MSG_OSD_MAP containing a crush map with at least one bucket has two fields holding the bucket algorithm. If the values in these two fields differ, an out-of-bounds access can occur. This is the case because the first algorithm field (alg) is used to allocate the correct amount of memory for a bucket of this type, while the second algorithm field inside the bucket (b->alg) is used in the subsequent processing. This patch fixes the issue by adding a check that compares alg and b->alg and aborts the processing in case they differ. Furthermore, b->alg is set to 0 in this case, because the destruction of the crush map also uses this field to determine the bucket type, which can again result in an out-of-bounds access when trying to free the memory pointed to by the fields of the bucket. To correctly free the memory allocated for the bucket in such a case, the	2026-06-24	9.8	CVE-2026-52955

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	corresponding call to kfree is moved from the algorithm-specific crush_destroy_bucket functions to the generic crush_destroy_bucket().			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: Fix potential out-of-bounds access in osdmap_decode() When decoding osd_state and osd_weight from an incoming osdmap in osdmap_decode(), both are decoded for each osd, i.e., map->max_osd times. The ceph_decode_need() check only accounts for sizeof(*map->osd_weight) once. This can potentially result in an out-of-bounds memory access if the incoming message is corrupted such that the max_osd value exceeds the actual content of the osdmap message. This patch fixes the issue by changing the corresponding part in the ceph_decode_need() check to account for map->max_osd*sizeof(*map->osd_weight).	2026-06-24	9.1	CVE-2026-52958
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: usb: rtl8150: fix use-after-free in rtl8150_start_xmit() syzbot reported a KASAN slab-use-after-free read in rtl8150_start_xmit() when accessing skb->len for tx statistics after usb_submit_urb() has been called: BUG: KASAN: slab-use-after-free in rtl8150_start_xmit+0x71f/0x760 drivers/net/usb/rtl8150.c:712 Read of size 4 at addr ffff88810eb7a930 by task kworker/0:4/5226 The URB completion handler write_bulk_callback() frees the skb via dev_kfree_skb_irq(dev->tx_skb). The URB may complete on another CPU in softirq context before usb_submit_urb() returns in the submitter, so by the time the submitter reads skb->len the skb has already been queued to the per-CPU completion_queue and freed by net_tx_action(): CPU A (xmit) CPU B (USB completion softirq) -----> -----> dev->tx_skb = skb; usb_submit_urb() --+ -----> write_bulk_callback() dev_kfree_skb_irq(dev->tx_skb) net_tx_action() napi_skb_cache_put() <-- free netdev->stats.tx_bytes += skb->len; <-- UAF read Fix it by caching skb->len before submitting the URB and using the cached value when updating the tx_bytes counter. The pre-existing tx_bytes semantics are preserved: the counter tracks the original frame length (skb->len), not the ETH_ZLEN/USB-alignment padded "count" value that is handed to the device. Changing that would be a user-visible accounting change and is out of scope for this UAF fix.	2026-06-24	9.8	CVE-2026-52982
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_sip: don't use simple_strtoul Replace unsafe port parsing in epaddr_len(), ct_sip_parse_header_uri(), and ct_sip_parse_request() with a new sip_parse_port() helper that validates each digit against the buffer limit, eliminating the use of simple_strtoul() which assumes NUL-terminated strings. The previous code dereferenced pointers without bounds checks after sip_parse_addr() and relied on simple_strtoul() on non-NUL-terminated skb data. A port that reaches the buffer limit without a trailing character is also rejected as malformed. Also get rid of all simple_strtoul() usage in conntrack, prefer a stricter version instead. There are intentional changes: - Bail out if number is > UINT_MAX and indicate a failure, same for too long sequences. While we do accept 05535 as port 5535, we will not accept e.g. 'sip:10.0.0.1:005060'. While its syntactically valid under RFC 3261, we should restrict this to not waste cycles when presented with malformed packets with 64k '0' characters. - Force base 10 in ct_sip_parse_numerical_param(). This is used to fetch 'expire=' and 'rports='; both are expected to use base-10. - In nf_nat_sip.c, only accept the parsed value if its within the 1k-64k range. - epaddr_len now returns 0 if the port is invalid, as it already does for invalid ip addresses. This is intentional. nf_conntrack_sip performs lots of guesswork to find the right parts of the message to parse. Being stricter could break existing setups. Connection tracking helpers are designed to allow traffic to pass, not to block it. Based on an earlier patch from Jenny Guanni Qu <qguanni@gmail.com>.	2026-06-24	9.8	CVE-2026-52986
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: propagate nvmet_tcp_build_pdu_iovec() errors to its callers Currently,	2026-06-24	9.8	CVE-2026-52989

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	when <code>nvmet_tcp_build_pdu_iovec()</code> detects an out-of-bounds PDU length or offset, it triggers <code>nvmet_tcp_fatal_error(cmd->queue)</code> and returns early. However, because the function returns void, the callers are entirely unaware that a fatal error has occurred and that the <code>cmd->recv_msg.msg_iter</code> was left uninitialized. Callers such as <code>nvmet_tcp_handle_h2c_data_pdu()</code> proceed to blindly overwrite the queue state with <code>queue->rcv_state = NVMET_TCP_RECV_DATA</code> . Consequently, the socket receiving loop may attempt to read incoming network data into the uninitialized iterator. Fix this by shifting the error handling responsibility to the callers.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: <code>tipc</code> : fix double-free in <code>tipc_buf_append()</code> <code>tipc_msg_validate()</code> can potentially reallocate the skb it is validating, freeing the old one. In <code>tipc_buf_append()</code> , it was being called with a pointer to a local variable which was a copy of the caller's skb pointer. If the skb was reallocated and validation subsequently failed, the error handling path would free the original skb pointer, which had already been freed, leading to double-free. Fix this by checking if <code>head</code> now points to a newly allocated reassembled skb. If it does, reassign <code>*headbuf</code> for later freeing operations.	2026-06-24	9.8	CVE-2026-52993
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: <code>netfilter</code> : <code>nfnetlink_osf</code> : fix out-of-bounds read on option matching In <code>nf_osf_match()</code> , the <code>nf_osf_hdr_ctx</code> structure is initialized once and passed by reference to <code>nf_osf_match_one()</code> for each fingerprint checked. During TCP option parsing, <code>nf_osf_match_one()</code> advances the shared <code>ctx->optp</code> pointer. If a fingerprint perfectly matches, the function returns early without restoring <code>ctx->optp</code> to its initial state. If the user has configured <code>NF_OSF_LOGLEVEL_ALL</code> , the loop continues to the next fingerprint. However, because <code>ctx->optp</code> was not restored, the next call to <code>nf_osf_match_one()</code> starts parsing from the end of the options buffer. This causes subsequent matches to read garbage data and fail immediately, making it impossible to log more than one match or logging incorrect matches. Instead of using a shared <code>ctx->optp</code> pointer, pass the context as a constant pointer and use a local pointer (<code>optp</code>) for TCP option traversal. This makes <code>nf_osf_match_one()</code> strictly stateless from the caller's perspective, ensuring every fingerprint check starts at the correct option offset.	2026-06-24	9.1	CVE-2026-52999
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: <code>netfilter</code> : <code>conntrack</code> : remove <code>sprintf</code> usage Replace it with <code>snprintf</code> , the buffer sizes are expected to be large enough to hold the result, no need for <code>snprintf</code> -overflow check. Increase buffer size in <code>mangle_content_len()</code> while at it. BUG: KASAN: stack-out-of-bounds in <code>vsnprintf+0xea5/0x1270</code> Write of size 1 at addr [...] <code>vsnprintf+0xea5/0x1270</code> <code>sprintf+0xb1/0xe0</code> <code>mangle_content_len+0x1ac/0x280</code> <code>nf_nat_sdp_session+0x1cc/0x240</code> <code>process_sdp+0x8f8/0xb80</code> <code>process_invite_request+0x108/0x2b0</code> <code>process_sip_msg+0x5da/0xf50</code> <code>sip_help_tcp+0x45e/0x780</code> <code>nf_confirm+0x34d/0x990</code> [...]	2026-06-24	9.8	CVE-2026-53002
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: <code>ipv6</code> : fix possible UAF in <code>icmpv6_rcv()</code> Caching <code>saddr</code> and <code>daddr</code> before <code>pskb_pull()</code> is problematic since <code>skb->head</code> can change. Remove these temporary variables: - We only access <code>&ipv6_hdr(skb)->saddr</code> and <code>&ipv6_hdr(skb)->daddr</code> when <code>net_dbg_ratelimited()</code> is called in the slow path. - Avoid potential future misuse after <code>pskb_pull()</code> call.	2026-06-24	9.8	CVE-2026-53006
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: <code>ksmbd</code> : fix use-after-free in <code>smb2_open</code> during durable reconnect In <code>smb2_open</code> , the call to <code>ksmbd_put_durable_fd(fp)</code> drops the reference to the durable file descriptor early during the durable reconnect process. If an error occurs subsequently (eg, <code>ksmbd_iov_pin_rsp</code> fails) or a scavenger accesses the file, it leads to a use-after-free when accessing <code>fp</code> properties (eg <code>fp-</code>	2026-06-24	9.8	CVE-2026-53010

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	>create_time). Move the single put to the end of the function below err_out2 so fp stays valid until smb2_open returns.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ocfs2/dlm: validate qr_numregions in dlm_match_regions() Patch series "ocfs2/dlm: fix two bugs in dlm_match_regions()". In dlm_match_regions(), the qr_numregions field from a DLM_QUERY_REGION network message is used to drive loops over the qr_regions buffer without sufficient validation. This series fixes two issues: - Patch 1 adds a bounds check to reject messages where qr_numregions exceeds O2NM_MAX_REGIONS. The o2net layer only validates message byte length; it does not constrain field values, so a crafted message can set qr_numregions up to 255 and trigger out-of-bounds reads past the 1024-byte qr_regions buffer. - Patch 2 fixes an off-by-one in the local-vs-remote comparison loop, which uses '<=' instead of '<', reading one entry past the valid range even when qr_numregions is within bounds. This patch (of 2): The qr_numregions field from a DLM_QUERY_REGION network message is used directly as loop bounds in dlm_match_regions() without checking against O2NM_MAX_REGIONS. Since qr_regions is sized for at most O2NM_MAX_REGIONS (32) entries, a crafted message with qr_numregions > 32 causes out-of-bounds reads past the qr_regions buffer. Add a bounds check for qr_numregions before entering the loops.	2026-06-24	9.1	CVE-2026-53043
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: memory: tegra124-emc: Fix dll_change check The code checking whether the specified memory timing enables DLL in the EMRS register was reversed. DLL is enabled if bit A0 is low. Fix the check.	2026-06-24	9.8	CVE-2026-53045
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free from async crypto on Qualcomm crypto engine ksmbd_crypt_message() sets a NULL completion callback on AEAD requests and does not handle the -EINPROGRESS return code from async hardware crypto engines like the Qualcomm Crypto Engine (QCE). When QCE returns -EINPROGRESS, ksmbd treats it as an error and immediately frees the request while the hardware DMA operation is still in flight. The DMA completion callback then dereferences freed memory, causing a NULL pointer crash: pc : qce_skcipher_done+0x24/0x174 lr : vchan_complete+0x230/0x27c ... el1h_64_irq+0x68/0x6c ksmbd_free_work_struct+0x20/0x118 [ksmbd] ksmbd_exit_file_cache+0x694/0xa4c [ksmbd] Use the standard crypto_wait_req() pattern with crypto_req_done() as the completion callback, matching the approach used by the SMB client in fs/smb/client/smb2ops.c. This properly handles both synchronous engines (immediate return) and async engines (-EINPROGRESS followed by callback notification).	2026-06-24	9.8	CVE-2026-53046
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: gfs2: add some missing log locking Function gfs2_logd() calls the log flushing functions gfs2_ail1_start(), gfs2_ail1_wait(), and gfs2_ail1_empty() without holding sdp->sd_log_flush_lock, but these functions require exclusion against concurrent transactions. To fix that, add a non-locking __gfs2_log_flush() function. Then, in gfs2_logd(), take sdp->sd_log_flush_lock before calling the above mentioned log flushing functions and __gfs2_log_flush().	2026-06-24	9.8	CVE-2026-53049
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: hisilicon/sec2 - prevent req used-after-free for sec During packet transmission, if the system is under heavy load, the hardware might complete processing the packet and free the request memory (req) before the transmission function finishes. If the software subsequently accesses this req, a use-after-free error will occur. The qp_ctx memory exists throughout the packet sending process, so replace the req with the qp_ctx.	2026-06-24	9.8	CVE-2026-53055

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: bcmgenet: fix racing timeout handler The bcmgenet_timeout handler tries to take down all tx queues when a single queue times out. This is over zealous and causes many race conditions with queues that are still chugging along. Instead lets only restart the timed out queue.	2026-06-24	9.8	CVE-2026-53086
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: bcmgenet: fix off-by-one in bcmgenet_put_txcb The write_ptr points to the next open tx_cb. We want to return the tx_cb that gets rewinded, so we must rewind the pointer first then return the tx_cb that it points to. That way the txcb can be correctly cleaned up.	2026-06-24	9.8	CVE-2026-53088
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: require Ethernet MAC header before using eth_hdr() `ip6t_eui64`, `xt_mac`, the `bitmap:ip,mac`, `hash:ip,mac`, and `hash:mac` ipset types, and `nf_log_syslog` access `eth_hdr(skb)` after either assuming that the skb is associated with an Ethernet device or checking only that the `ETH_HLEN` bytes at `skb_mac_header(skb)` lie between `skb->head` and `skb->data`. Make these paths first verify that the skb is associated with an Ethernet device, that the MAC header was set, and that it spans at least a full Ethernet header before accessing `eth_hdr(skb)`.	2026-06-25	9.4	CVE-2026-53131
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix the ACK parser to extract the SACK table for parsing Fix modification of the received skbuff in rxrpc_input_soft_acks() and a potential incorrect access of the buffer in a fragmented UDP packet (the packet would probably have to be deliberately pre-generated as fragmented) when AF_RXRPC tries to extract the contents of the SACK table by copying out the contents of the SACK table into a buffer before attempting to parse AF_RXRPC assumes that it can just call skb_condense() and then validly access the SACK table from skb->data and that it will be a flat buffer - but skb_condense() can silently fail to do anything under some circumstances. Note that whilst rxrpc_input_soft_acks() should be able to parse extended ACKs, the rest of AF_RXRPC doesn't currently support that. Further, there's then no need to call skb_condense() in rxrpc_input_ack(), so don't.	2026-06-25	9.8	CVE-2026-53151
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: inet: frags: fix use-after-free caused by the fqdir_pre_exit() flush On netns teardown, fqdir_pre_exit() walks the fqdir rhashtable and flushes every fragment queue that is not yet complete using inet_frag_queue_flush(). That helper frees all the skbs queued on the fragment queue but does not set INET_FRAG_COMPLETE, and leaves q->fragments_tail and q->last_run_head pointing at the freed skbs. The queue itself stays in the rhashtable. fqdir_pre_exit() first lowers high_thresh to 0 to stop new queue lookups, but it cannot stop a fragment that already obtained the queue through inet_frag_find() earlier and stalled just before taking the queue lock. Once that fragment resumes after the flush and takes the queue lock, it passes the INET_FRAG_COMPLETE check and then dereferences the freed fragments_tail. inet_frag_queue_insert() reads FRAG_CB() and ->len of that pointer and, on the append path, writes ->next_frag, causing a slab use-after-free. IPv6, nf_conntrack_reasm6 and 6lowpan reassembly share the same flush path and are affected as well. Reset rb_fragments, fragments_tail and last_run_head in inet_frag_queue_flush() so a flushed queue no longer points at the freed skbs. A fragment that resumes after the flush and takes the queue lock then finds an empty queue and starts a new run instead of dereferencing the freed fragments_tail. ip_frag_reinit() already performed this reset after its own flush, so drop the now duplicate code there.	2026-06-25	9.8	CVE-2026-53175
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: IB/isert: Reject login PDUs shorter than ISER_HEADERS_LEN In drivers/infiniband/ulp/isert/ib_isert.c, isert_login_recv_done() computes the login request payload length as wc->byte_len minus ISER_HEADERS_LEN with no lower bound, and login_req_len is a signed	2026-06-25	9.8	CVE-2026-53176

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	int. A remote iSER initiator can post a login Send work request carrying fewer than ISER_HEADERS_LEN (76) bytes, so the subtraction underflows and login_req_len becomes negative. isert_rx_login_req() then reads that negative length back into a signed int, takes size = min(rx_buf_len, MAX_KEY_VALUE_PAIRS), and because the min() is signed it keeps the negative value; the value is then passed as the memcpy() length and sign-extended to a multi-gigabyte size_t. The copy into the 8192-byte login->req_buf runs far out of bounds and faults, crashing the target node. The login phase precedes iSCSI authentication, so no credentials are required to reach this path. Reject any login PDU shorter than ISER_HEADERS_LEN before the subtraction, mirroring the existing early return on a failed work completion, so login_req_len can never go negative. The upper bound was already safe: a posted login buffer cannot deliver more than ISER_RX_PAYLOAD_SIZE, so the difference stays at or below MAX_KEY_VALUE_PAIRS and the existing min() clamps it; only the missing lower bound needs to be added.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/srp: bound SRP_RSP sense copy by the received length srp_process_rsp() copies sense data from rsp->data + resp_data_len, where resp_data_len is the full 32-bit value supplied by the SRP target and is never checked against the number of bytes actually received (wc->byte_len). The copy length is bounded to SCSI_SENSE_BUFFERSIZE, so at most 96 bytes are copied, but the source offset is not bounded. A malicious or compromised SRP target on the InfiniBand/RoCE fabric that the initiator has logged into can return an SRP_RSP with SRP_RSP_FLAG_SNSVALID set and a large resp_data_len. The receive buffer is allocated at the target-chosen max_ti_iu_len, so the source of the sense copy lands past the bytes actually received; with resp_data_len near 0xFFFFFFFF it is gigabytes past the buffer and the read faults. Copy the sense data only if it has not been truncated, that is, only if the response header, the response data, and the sense region fit within the bytes actually received; otherwise drop the sense and log. The in-tree iSER and NVMe-RDMA receive paths already bound their parse by wc->byte_len; this brings ib_srp into line with them.	2026-06-25	9.1	CVE-2026-53186
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: mvpp2: refill RX buffers before XDP or skb use The RX error path returns the current descriptor buffer to the hardware BM pool. That is only valid while the driver still owns the buffer. mvpp2_rx_refill() can fail after the current buffer has been handed to XDP or attached to an skb. In those cases mvpp2_run_xdp() may have recycled, redirected, or queued the page for XDP_TX, and an skb free also retires the data buffer. Returning such a buffer to BM lets hardware DMA into memory that is no longer owned by the RX ring. Refill the BM pool before handing the current buffer to XDP or to the skb. If the allocation fails there, drop the packet and return the still-owned current buffer to BM, preserving the pool depth. Once the refill succeeds, later local drops retire/free the current buffer instead of returning it to BM.	2026-06-25	9.8	CVE-2026-53215
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: mvpp2: limit XDP frame size to the RX buffer mvpp2 has short and long BM pools, and short pool buffers can be smaller than PAGE_SIZE. The XDP path nevertheless initializes every xdp_buff with PAGE_SIZE as frame size. XDP helpers use frame_sz to validate tail growth and to derive the hard end of the data area. Advertising PAGE_SIZE for short buffers can let bpf_xdp_adjust_tail() grow a packet past the real allocation, corrupting memory or later tripping skb tailroom checks. Initialize the XDP buffer with bm_pool->frag_size so XDP tailroom matches the actual buffer backing the packet.	2026-06-25	9.8	CVE-2026-53216
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ip6_vti: fix incorrect tunnel matching in vti6_tnl_lookup() In vti6_tnl_lookup(),	2026-06-25	9.8	CVE-2026-53221

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	when an exact match for a tunnel fails, the code falls back to searching for wildcard tunnels: - Tunnels matching the packet's local address, with any remote address wildcard remote). - Tunnels matching the packet's remote address, with any local address (wildcard local). However, vti6 stores all these different types of tunnels in the same hash table (ip6n->tnls_r_l) prone to hash collisions. The bug is that the fallback search loops in vti6_tnl_lookup() were missing checks to ensure that the candidate tunnel actually has a wildcard address.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: validate embedded INIT chunk and address list lengths in cookie sctp_unpack_cookie() only checked that the embedded INIT chunk length did not exceed the remaining cookie payload, but did not ensure that the INIT chunk is large enough to contain a complete INIT header. A malformed COOKIE_ECHO can therefore carry a truncated INIT chunk whose length field is smaller than sizeof(struct sctp_init_chunk). Later, sctp_process_init() accesses INIT parameters unconditionally, which may lead to out-of-bounds reads. In addition, raw_addr_list_len is not fully validated against the remaining cookie payload. When cookie authentication is disabled, an attacker can supply an oversized raw_addr_list_len and cause sctp_raw_to_bind_addrs() to read beyond the end of the cookie. The address parser also lacks sufficient bounds checks for parameter headers and lengths, allowing malformed address parameters to trigger out-of-bounds reads. Fix this by: - requiring the embedded INIT chunk length to be at least sizeof(struct sctp_init_chunk); - validating that the INIT chunk and raw address list together fit within the cookie payload; - verifying sufficient data exists for each address parameter header and payload before parsing it. Note that sctp_verify_init() must be called after sctp_unpack_cookie() and before sctp_process_init() when cookie authentication is disabled. This will be addressed in a separate patch.	2026-06-25	9.1	CVE-2026-53224
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: fix uninit-value in __sctp_rcv_asconf_lookup() __sctp_rcv_asconf_lookup() in net/sctp/input.c only checks that the ASCONF chunk can hold the ADDIP header and a parameter header, then calls af->from_addr_param(), which reads the full address (16 bytes for IPv6) trusting the parameter's declared length. An unauthenticated peer can send a truncated trailing ASCONF chunk that declares an IPv6 address parameter but stops after the 4-byte parameter header; reached from the no-association lookup path, from_addr_param() then reads uninitialized bytes past the parameter. Impact: an unauthenticated SCTP peer makes the receive path read up to 16 bytes of uninitialized memory past a truncated ASCONF address parameter. The sibling __sctp_rcv_init_lookup() bounds parameters with sctp_walk_params(); this path open-codes the fetch and omits the bound. Verify the whole address parameter lies within the chunk before from_addr_param() reads it, the same class of fix as commit 51e5ad549c43 ("net: sctp: fix KMSAN uninit-value in sctp_inq_pop").	2026-06-25	9.1	CVE-2026-53225
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: sit: reload inner IPv6 header after GSO offloads ipip6_tunnel_xmit() caches the inner IPv6 header pointer at function entry and continues using it after iptunnel_handle_offloads(). For GSO skbs, iptunnel_handle_offloads() calls skb_header_unclone(). When the skb header is cloned, skb_header_unclone() can call pskb_expand_head(), which may move the skb head. The pskb_expand_head() contract requires pointers into the skb header to be reloaded after the call. If the later skb_realloc_headroom() branch is not taken, SIT uses the stale iph6 pointer to read the inner hop limit and DS field. That can read from a freed skb head after the old head's remaining clone is released. Reload iph6 after the offload helper succeeds and before subsequent reads from the inner IPv6 header. Keep the	2026-06-25	9.8	CVE-2026-53228

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	existing reload after skb_realloc_headroom(), since that branch can also replace the skb.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: validate cached peer INIT chunk length in COOKIE_ECHO processing When a listening SCTP server processes a COOKIE_ECHO chunk, the cached peer INIT chunk embedded after the cookie is parsed and its parameters are later walked by sctp_process_init() using sctp_walk_params(). However, the chunk header length of this cached INIT chunk was not validated against the remaining buffer in the COOKIE_ECHO payload. If the length field is inflated, the parameter walk can run beyond the actual received data, leading to out-of-bounds reads and potential memory corruption during later parameter handling (e.g. STATE_COOKIE processing and kmemdup() copies). Add a bounds check in sctp_unpack_cookie() to ensure the cached INIT chunk length does not exceed the available data in the COOKIE_ECHO buffer before it is used.	2026-06-25	9.8	CVE-2026-53246
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: mtk_eth_soc: Fix use-after-free in metadata dst teardown mtk_free_dev() calls metadata_dst_free() which frees the metadata_dst with kfree() immediately, bypassing the RCU grace period. In the RX path, skb_dst_set_noref() sets a non-refcounted pointer from the skb to the metadata_dst. This function requires RCU read-side protection and the dst must remain valid until all RCU readers complete. Since metadata_dst_free() calls kfree() directly, a use-after-free can occur if any skb still holds a noref pointer to the dst when the driver tears it down. Replace metadata_dst_free() with dst_release() which properly goes through the refcount path: when the refcount drops to zero, it schedules the actual free via call_rcu_hurry(), ensuring all RCU readers have completed before the memory is freed.	2026-06-25	9.8	CVE-2026-53247
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Add preempt_{disable,enable}_nested() in reqsk_queue_hash_req(). syzbot reported a weird reqsk->rsk_refcnt underflow in __inet_csk_reqsk_queue_drop(). The captured reqsk_put() in __inet_csk_reqsk_queue_drop() is called only when it successfully removes reqsk from ehash. Moreover, reqsk_timer_handler() calls another reqsk_put() after that. This indicates that the reqsk was missing both refcnts for ehash and the timer itself. Since all the syzbot reports had PREEMPT_RT enabled, the only possible scenario is that reqsk_queue_hash_req() is preempted after mod_timer() and before refcount_set(), and then the timer triggered after 1s aborts the reqsk due to its listener's close(). Let's wrap mod_timer() and refcount_set() with preempt_disable_nested() and preempt_enable_nested(). Note that inet_ehash_insert() holds the normal spin_lock() (mutex in PREEMPT_RT), so it must be called outside of preempt_disable_nested(), but this is fine. The lookup path just ignores 0 sk_refcnt entries in ehash and tries to create another reqsk, but this will fail at inet_ehash_insert(). [0]: refcount_t: underflow; use-after-free. WARNING: lib/refcount.c:28 at refcount_warn_saturate+0xb2/0x110 lib/refcount.c:28, CPU#0: ktimers/0/16 Modules linked in: CPU: 0 UID: 0 PID: 16 Comm: ktimers/0 Tainted: G L syzkaller #0 PREEMPT_{RT,(full)} Tainted: [L]=SOFTLOCKUP Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 04/18/2026 RIP: 0010:refcount_warn_saturate+0xb2/0x110 lib/refcount.c:28 Code: e4 7d d1 0a 67 48 0f b9 3a eb 4a e8 38 3d 23 fd 48 8d 3d e1 7d d1 0a 67 48 0f b9 3a eb 37 e8 25 3d 23 fd 48 8d 3d de 7d d1 0a <67> 48 0f b9 3a eb 24 e8 12 3d 23 fd 48 8d 3d db 7d d1 0a 67 48 0f RSP: 0000:ffffc90000157948 EFLAGS: 00010246 RAX: ffffffff84a1301b RBX: 0000000000000003 RCX: ffff88801ca98000 RDX: 0000000000000100 RSI: 0000000000000000 RDI: ffffffff8f72ae00 RBP: ffffffff99ae3b01 R08: ffff88801ca98000 R09: 0000000000000005 R10: 0000000000000100 R11: 0000000000000004 R12: ffff8880425ef568 R13: ffff8880425ef4f8 R14:	2026-06-25	9.8	CVE-2026-53260

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ffff8880425ef578 R15: 0000000000000000 FS: 0000000000000000(0000) GS:ffff888126386000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f7b46710e9c CR3: 000000000dbb6000 CR4: 00000000003526f0 Call Trace: <TASK> __refcount_sub_and_test include/linux/refcount.h:400 [inline] __refcount_dec_and_test include/linux/refcount.h:432 [inline] refcount_dec_and_test include/linux/refcount.h:450 [inline] reqsk_put include/net/request_sock.h:136 [inline] __inet_csk_reqsk_queue_drop+0x3ce/0x440 net/ipv4/inet_connection_sock.c:1007 reqsk_timer_handler+0x651/0xdf0 net/ipv4/inet_connection_sock.c:1137 call_timer_fn+0x192/0x5e0 kernel/time/timer.c:1748 expire_timers kernel/time/timer.c:1799 [inline] __run_timers kernel/time/timer.c:2374 [inline] __run_timer_base+0x6a3/0x9f0 kernel/time/timer.c:2386 run_timer_base kernel/time/timer.c:2395 [inline] run_timer_softirq+0x67/0x170 kernel/time/timer.c:2403 handle_softirqs+0x1de/0x6d0 kernel/softirq.c:622 __do_softirq kernel/softirq.c:656 [inline] run_ktimerd+0x69/0x100 kernel/softirq.c:1151 smpboot_thread_fn+0x541/0xa50 kernel/smpboot.c:160 kthread+0x388/0x470 kernel/kthread.c:436 ret_from_fork+0x514/0xb70 arch/x86/kernel/process.c:158 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 </TASK>			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ocfs2/dlm: fix off-by-one in dlm_match_regions() region comparison The local-vs-remote region comparison loop uses '<=' instead of '<', causing it to read one entry past the valid range of qr_regions. The other loops in the same function correctly use '<'. Fix the loop condition to use '<' for consistency and correctness.	2026-06-26	9.8	CVE-2026-53309
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: serialize accept_q access bt_sock_poll() walks the accept queue without synchronization, while child teardown can unlink the same socket and drop its last reference. The unsynchronized accept queue walk has existed since the initial Bluetooth import. Protect accept_q with a dedicated lock for queue updates and polling. Also rework bt_accept_dequeue() to take temporary child references under the queue lock before dropping it and locking the child socket.	2026-06-24	8.8	CVE-2026-52918
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: xt_policy: fix strict mode inbound policy matching match_policy_in() walks sec_path entries from the last transform to the first one, but strict policy matching needs to consume info->pol[] in the same forward order as the rule layout. Derive the strict-match policy position from the number of transforms already consumed so that multi-element inbound rules are matched consistently.	2026-06-24	8.3	CVE-2026-52920
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: tvlv: reject oversized TVLV packets batadv_tvlv_container_ogm_append() builds a TVLV packet section from the tvlv.container_list. The total size of this section is computed by batadv_tvlv_container_list_size(), which sums the sizes of all registered containers. The return type and accumulator in batadv_tvlv_container_list_size() were u16. If the accumulated size exceeds U16_MAX, the value wraps around, causing the subsequent allocation in batadv_tvlv_container_ogm_append() to be undersized. The memcpy-style copy that follows would then write beyond the end of the allocated buffer, corrupting kernel memory. Fix this by widening the return type of batadv_tvlv_container_list_size() to size_t. In batadv_tvlv_container_ogm_append(), check the computed length against U16_MAX before proceeding, and bail out as if the allocation had failed when the limit is exceeded.	2026-06-24	8.8	CVE-2026-52934

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iommu: Fix WARN_ON in __iommu_group_set_domain_nofail() due to reset In __iommu_group_set_domain_internal(), concurrent domain attachments are rejected when any device in the group is recovering. This is necessary to fence concurrent attachments to a multi-device group where devices might share the same RID due to PCI DMA alias quirks, but triggers the WARN_ON in __iommu_group_set_domain_nofail(). Other IOMMU_SET_DOMAIN_MUST_SUCCEED callers in detach/teardown paths, such as __iommu_group_set_core_domain and __iommu_release_dma_ownership, should not be rejected, as the domain would be freed anyway in these nofail paths while group->domain is still pointing to it. So pci_dev_reset_iommu_done() could trigger a UAF when re-attaching group->domain. Honor the IOMMU_SET_DOMAIN_MUST_SUCCEED flag, allowing the callers through the group->recovery_cnt fence, so as to update the group->domain pointer. Instead add a gdev->blocked check in the device iteration loop, to prevent any concurrent per-device detachment.	2026-06-24	8.8	CVE-2026-52952
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: smb/client: fix possible infinite loop and oob read in symlink_data() On 32-bit architectures, the infinite loop is as follows: len = p->ErrorDataLength == 0xffffffff u8 *next = p->ErrorContextData + len next == p On 32-bit architectures, the out-of-bounds read is as follows: len = p->ErrorDataLength == 0xffffffff u8 *next = p->ErrorContextData + len next == (u8 *)p - 8	2026-06-24	8.1	CVE-2026-52967
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iommu/amd: Fix clone_alias() to use the original device's devid Currently clone_alias() assumes first argument (pdev) is always the original device pointer. This function is called by pci_for_each_dma_alias() which based on topology decides to send original or alias device details in first argument. This meant that the source devid used to look up and copy the DTE may be incorrect, leading to wrong or stale DTE entries being propagated to alias device. Fix this by passing the original pdev as the opaque data argument to both the direct clone_alias() call and pci_for_each_dma_alias(). Inside clone_alias(), retrieve the original device from data and compute devid from it.	2026-06-24	8.8	CVE-2026-53053
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iommu/riscv: Add IOTINVAL after updating DDT/PDT entries Add riscv_iommu_iotdir_iotinval() to perform required TLB and context cache invalidations after updating DDT or PDT entries, as mandated by the RISC-V IOMMU specification (Section 6.3.1 and 6.3.2).	2026-06-24	8.8	CVE-2026-53057
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: l2cap: Add missing chan lock in l2cap_ecred_reconf_rsp l2cap_ecred_reconf_rsp() calls l2cap_chan_del() without holding l2cap_chan_lock(). Every other l2cap_chan_del() caller in the file acquires the lock first. A remote BLE device can send a crafted L2CAP ECREd reconfiguration response to corrupt the channel list while another thread is iterating it. Add l2cap_chan_hold() and l2cap_chan_lock() before l2cap_chan_del(), and l2cap_chan_unlock() and l2cap_chan_put() after, matching the pattern used in l2cap_ecred_conn_rsp() and l2cap_conn_del().	2026-06-24	8.8	CVE-2026-53071
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: fix locking in hci_conn_request_evt() with HCI_PROTO_DEFER When protocol sets HCI_PROTO_DEFER, hci_conn_request_evt() calls hci_connect_cfm(conn) without hdev->lock. Generally hci_connect_cfm() assumes it is held, and if conn is deleted concurrently -> UAF. Only SCO and ISO set HCI_PROTO_DEFER and only for defer setup listen, and HCI_EV_CONN_REQUEST is not generated for ISO. In the non-deferred listening socket code paths, hci_connect_cfm(conn) is called with hdev->lock held. Fix by holding the lock.	2026-06-24	8.8	CVE-2026-53072

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ppp: require CAP_NET_ADMIN in target netns for unattached ioctls /dev/ppp open is currently authorized against file->f_cred->user_ns, while unattached administrative ioctls operate on current->nsproxy->net_ns. As a result, a local unprivileged user can create a new user namespace with CLONE_NEWUSER, gain CAP_NET_ADMIN only in that new user namespace, and still issue PPPIOCNEWUNIT, PPPIOCATTACH, or PPPIOCATTCHAN against an inherited network namespace. Require CAP_NET_ADMIN in the user namespace that owns the target network namespace before handling unattached PPP administrative ioctls. This preserves normal pppd operation in the network namespace it is actually privileged in, while rejecting the usersns-only inherited-netns case.	2026-06-24	8.8	CVE-2026-53075
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: pull headers in qdisc_pkt_len_segs_init() Most ndo_start_xmit() methods expects headers of gso packets to be already in skb->head. net/core/tso.c users are particularly at risk, because tso_build_hdr() does a memcpy(hdr, skb->data, hdr_len); qdisc_pkt_len_segs_init() already does a dissection of gso packets. Use pskb_may_pull() instead of skb_header_pointer() to make sure drivers do not have to reimplement this. Some malicious packets could be fed, detect them so that we can drop them sooner with a new SKB_DROP_REASON_SKB_BAD_GSO drop_reason.	2026-06-24	8.4	CVE-2026-53091
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Validate XDomain request packet size before type cast tb_xdp_handle_request() casts the received packet buffer to protocol-specific structs without verifying that the allocation is large enough for the target type. A peer can send a minimal XDomain packet that passes the generic header length check but is shorter than the struct accessed after the cast, causing out-of-bounds reads from the kmemdup allocation. Plumb the packet length through xdomain_request_work and validate it against the expected struct size before each cast.	2026-06-25	8.1	CVE-2026-53147
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/ethosu: reject DMA commands with uninitialized length cmd_state_init() initializes the command state with memset(0xff), leaving dma->len at U64_MAX to signal missing setup. The only setter is NPU_SET_DMA0_LEN; if userspace omits this command and issues NPU_OP_DMA_START, dma->len remains U64_MAX. In dma_length(), a positive stride added to U64_MAX wraps to a small value. With size0 == 1, check_mul_overflow() does not trigger and dma_length() returns 0 instead of U64_MAX. The caller's U64_MAX check then passes, region_size[] stays 0, and the bounds check in ethosu_job.c is bypassed, allowing hardware to execute DMA with stale physical addresses. Fix by checking for U64_MAX at the start of dma_length() before any arithmetic, consistent with the sentinel value used throughout the driver to detect uninitialized fields.	2026-06-25	8.8	CVE-2026-53170
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/ethosu: fix arithmetic issues in dma_length() dma_length() derives DMA region usage from command stream values and updates region_size[]: len = ((len + stride[0]) * size0 + stride[1]) * size1 region_size[region] = max(..., len + dma->offset) Several arithmetic issues can corrupt the derived region size: - signed stride values may underflow when added to len - intermediate multiplications may overflow - len + dma->offset may overflow during region_size updates - dma_length() error returns were not validated by the caller region_size[] is later used by ethosu_job.c to validate command stream accesses against GEM buffer sizes. Arithmetic wraparound can therefore under-report region usage and bypass the bounds validation. Fix by validating signed additions, using overflow helpers for multiplications and offset updates, and propagating dma_length() failures to the caller.	2026-06-25	8.8	CVE-2026-53171
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: staging: rtl8723bs: rtw_mlme: add bounds checks before ie_length subtraction Add	2026-06-25	8.1	CVE-2026-53178

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	guards to ensure ie_length is large enough before subtracting fixed IE offsets to prevent unsigned integer underflow.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/core: Validate the passed in fops for ib_get_ucaps() Sashiko pointed out it is not safe to rely only on the devt because char/block alias so if the user finds a block device with the same dev_t it can masquerade as a ucaps cdev fd. Test the f_ops to only accept authentic cdevs.	2026-06-25	8.8	CVE-2026-53188
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free of a deferred file_lock on double SMB2_CANCEL A deferred byte-range lock (an SMB2_LOCK that blocks) registers an async work on conn->async_requests via setup_async_work(), with cancel_fn = smb2_remove_blocked_lock and cancel_argv[0] pointing at the struct file_lock. When the request is cancelled, the worker frees the file_lock with locks_free_lock() and takes the cancelled early-exit, which "goto out"s and never reaches release_async_work() -- the only site that unlinks the work from conn->async_requests and clears cancel_fn/cancel_argv. The work therefore stays matchable on async_requests with a live cancel_fn pointing at the freed file_lock, until connection teardown finally runs release_async_work(). smb2_cancel() fires cancel_fn unconditionally with no state guard, so a second SMB2_CANCEL for the same AsyncId, arriving in that window, re-runs smb2_remove_blocked_lock() on the freed file_lock -- a slab use-after-free: BUG: KASAN: slab-use-after-free in __locks_delete_block __locks_delete_block locks_delete_block ksmbd_vfs_posix_lock_unblock smb2_remove_blocked_lock smb2_cancel <- 2nd SMB2_CANCEL fires cancel_fn handle_ksmbd_work Allocated by ...: locks_alloc_lock <- smb2_lock Freed by ...: locks_free_lock <- smb2_lock (cancelled branch) ... cache file_lock_cache of size 192 Reproduced on mainline with KASAN by an authenticated SMB client. Skip a work whose state is already KSMDBD_WORK_CANCELLED so its cancel callback cannot be fired a second time.	2026-06-25	8.8	CVE-2026-53198
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: nv: Fix handling of XN[0] when !FEAT_XNX XN has already been extracted from its bitfield position so using FIELD_PREP() on the mask that clears XN[0] is completely broken, having the effect of unconditionally granting execute permissions... Fix the obvious mistake by manipulating the right bit.	2026-06-25	8.8	CVE-2026-53200
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: mvpp2: sync RX data at the hardware packet offset mvpp2 programs the RX queue packet offset, so hardware writes received data at dma_addr + MVPP2_SKB_HEADROOM. The current CPU sync starts at dma_addr and only covers rx_bytes + MVPP2_MH_SIZE bytes, which syncs the unused headroom and misses the same number of bytes at the packet tail. On non-coherent DMA systems this can leave the CPU reading stale cache contents for the end of the received frame. Use dma_sync_single_range_for_cpu() with MVPP2_SKB_HEADROOM as the range offset so the sync covers the Marvell header and packet data actually written by hardware.	2026-06-25	8.6	CVE-2026-53217
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix slab-out-of-bounds in mlx5_query_nic_vport_mac_list mlx5_query_nic_vport_mac_list() sizes its firmware command buffer using the PF's log_max_current_uc/mc_list capabilities. When querying a VF vport with a larger configured max (via devlink), the firmware response can overflow this buffer: BUG: KASAN: slab-out-of-bounds in mlx5_query_nic_vport_mac_list+0x453/0x4c0 [mlx5_core] Read of size 4 at addr ff1100013ffc8a12 by task kworker/u96:2/385 CPU: 12 UID: 0 PID: 385 Comm: kworker/u96:2 Not tainted 7.0.0-rc6+ #1 PREEMPT Hardware name: QEMU Standard PC (Q35 + ICH9, 2009) Workqueue: mlx5_esw_wq esw_vport_change_handler [mlx5_core] Call Trace: <TASK> dump_stack_lvl+0x69/0xa0 print_report+0x176/0x4e4	2026-06-25	8.7	CVE-2026-53230

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	kasan_report+0xc8/0x100 mlx5_query_nic_vport_mac_list+0x453/0x4c0 [mlx5_core] esw_update_vport_addr_list+0x2e3/0xda0 [mlx5_core] esw_vport_change_handle_locked+0xa1f/0x1060 [mlx5_core] esw_vport_change_handler+0x6a/0x90 [mlx5_core] process_one_work+0x87f/0x15e0 worker_thread+0x62b/0x1020 kthread+0x375/0x490 ret_from_fork+0x4dc/0x810 ret_from_fork_asm+0x11/0x20 </TASK> Fix by querying the vport's own HCA caps to size the buffer correctly. Refactor the function to allocate and return the MAC list internally, removing the caller's dependency on knowing the correct max.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: phy: clean the sfp upstream if phy probing fails Sashiko reported that we don't call sfp_bus_del_upstream() in the probe failure path, so let's add it, otherwise the sfp-bus is left with a dangling 'upstream' field, that may be used later on during SFP events. This issue existed before the generic phylib sfp support, back when drivers were calling phy_sfp_probe themselves.	2026-06-25	8.8	CVE-2026-53232
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: iptfs: fix use-after-free on first_skb in __input_process_payload __input_process_payload() stores first_skb into xtfs->ra_newskb under drop_lock when starting partial reassembly, then unlocks and breaks out of the processing loop. The post-loop check reads xtfs->ra_newskb without the lock to decide whether first_skb is still owned: if (first_skb && first_iphlen && !defer && first_skb != xtfs->ra_newskb) Between spin_unlock and this read, a concurrent CPU running iptfs_reassem_cont() (or the drop_timer hrtimer) can complete reassembly, NULL xtfs->ra_newskb, and free the skb. The check then evaluates first_skb != NULL as true, and pskb_trim/ip_summed/consume_skb operate on the freed skb - a use-after-free in skbuff_head_cache. Replace the unlocked read with a local bool that records whether first_skb was handed to the reassembly state in the current call. The flag is set after the existing spin_unlock, before the break, using the pointer equality that is stable at that point (first_skb == skb iff first_skb was stored in ra_newskb).	2026-06-25	8.8	CVE-2026-53240
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: airoha: Fix use-after-free in metadata dst teardown airoha_metadata_dst_free() runs metadata_dst_free() which frees the metadata_dst with kfree() immediately, bypassing the RCU grace period. In the RX path, skb_dst_set_noref() sets a non-refcounted pointer from the skb to the metadata_dst. This function requires RCU read-side protection and the dst must remain valid until all RCU readers complete. Since metadata_dst_free() calls kfree() directly, an use-after-free can occur if any skb still holds a noref pointer to the dst when the driver tears it down. Replace metadata_dst_free() with dst_release() which properly goes through the refcount path: when the refcount drops to zero, it schedules the actual free via call_rcu_hurry(), ensuring all RCU readers have completed before the memory is freed.	2026-06-25	8.8	CVE-2026-53248
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: RFCOMM: validate skb length in MCC handlers The RFCOMM MCC handlers cast skb->data to protocol-specific structs without validating skb->len first. A malicious remote device can send truncated MCC frames and trigger out-of-bounds reads in these handlers. Fix this by using skb_pull_data() to validate and access the required data before dereferencing it. rfcomm_rcv_rpn() requires special handling since ETSI TS 07.10 allows 1-byte RPN requests. Handle this by validating only the DLCI byte first, and validating the full struct only when len > 1.	2026-06-25	8.1	CVE-2026-53254
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: RFCOMM: hold listener socket in rfcomm_connect_ind() rfcomm_get_sock_by_channel() scans rfcomm_sk_list under the list lock, but returns the selected listener after dropping that lock without taking a	2026-06-25	8	CVE-2026-53256

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	reference. rfcomm_connect_ind() then locks the listener, queues a child socket on it, and may notify it after unlocking it. The buggy scenario involves two paths, with each column showing the order within that path: rfcomm_connect_ind(): listener close: 1. Find parent in 1. close() enters rfcomm_get_sock_by_channel() rfcomm_sock_release(). 2. Drop rfcomm_sk_list.lock 2. rfcomm_sock_shutdown() without pinning parent. closes the listener. 3. Call lock_sock(parent) and 3. rfcomm_sock_kill() bt_accept_enqueue(parent, unlinks and puts parent. sk, true). 4. Read parent flags and may 4. parent can be freed. call sk_state_change(). If close wins the race, parent can be freed before rfcomm_connect_ind() reaches lock_sock(), bt_accept_enqueue(), or the deferred-setup callback. Take a reference on the listener before leaving rfcomm_sk_list.lock. After lock_sock() succeeds, recheck that it is still in BT_LISTEN before queueing a child, cache the deferred-setup bit while the parent is locked, and drop the reference after the last parent use. KASAN reported a slab-use-after-free in lock_sock_nested() from rfcomm_connect_ind(), with the freeing stack going through rfcomm_sock_kill() and rfcomm_sock_release().			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: bridge: make ebt_snat ARP rewrite writable The ebttables SNAT target keeps the Ethernet source address rewrite behind skb_ensure_writable(skb, 0). This is intentional: at the bridge ebttables hooks the Ethernet header is addressed through skb_mac_header()/eth_hdr(), while skb->data points at the Ethernet payload. Asking skb_ensure_writable() for ETH_HLEN bytes would check the payload, not the Ethernet header, and would reintroduce the small packet regression fixed by commit 63137bc5882a. However, the optional ARP sender hardware address rewrite is different. It writes through skb_store_bits() at an offset relative to skb->data: skb_store_bits(skb, sizeof(struct arphdr), info->mac, ETH_ALEN) skb_header_pointer() only safely reads the ARP header; it does not make the later sender hardware address range writable. If that range is still held in a nonlinear skb fragment backed by a splice-imported file page, skb_store_bits() maps the frag page and copies the new MAC address directly into it. Ensure the ARP SHA range is writable before reading the ARP header and before calling skb_store_bits().	2026-06-25	8.8	CVE-2026-53266
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: conntrack_irc: fix possible out-of-bounds read When parsing fails after we've matched the command string we should bail out instead of trying to match a different command. This helper should be deprecated, given prevalence of TLS I doubt it has any relevance in 2026.	2026-06-25	8.2	CVE-2026-53268
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: mcast: Fix use-after-free when processing MLD queries When processing an MLD query, a pointer to the multicast group address is retrieved when initially parsing the packet. This pointer is later dereferenced without being reloaded despite the fact that the skb header might have been reallocated following the pskb_may_pull() calls, leading to a use-after-free [1]. Fix by copying the multicast group address when the packet is initially parsed. [1] BUG: KASAN: slab-use-after-free in __mld_query_work (net/ipv6/mcast.c:1512) Read of size 8 at addr ffff8881154b8e90 by task kworker/4:1/118 Workqueue: mld mld_query_work Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:94 lib/dump_stack.c:120) print_address_description.constprop.0 (mm/kasan/report.c:378) print_report (mm/kasan/report.c:482) kasan_report (mm/kasan/report.c:595) __mld_query_work (net/ipv6/mcast.c:1512) mld_query_work (net/ipv6/mcast.c:1563) process_one_work (kernel/workqueue.c:3314) worker_thread (kernel/workqueue.c:3397) kernel/workqueue.c:3478 kthread (kernel/kthread.c:436) ret_from_fork (arch/x86/kernel/process.c:158) ret_from_fork_asm (arch/x86/entry/entry_64.S:245) </TASK> [...] Freed by task 118:	2026-06-25	8.8	CVE-2026-53275

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	kasan_save_stack (mm/kasan/common.c:57) kasan_save_track (mm/kasan/common.c:78) kasan_save_free_info (mm/kasan/generic.c:584) __kasan_slab_free (mm/kasan/common.c:253) mm/kasan/common.c:285) kfree (/include/linux/kasan.h:235) mm/slab.c:2689 mm/slab.c:6251 mm/slab.c:6566) pskb_expand_head (net/core/skbuff.c:2335) __pskb_pull_tail (net/core/skbuff.c:2878) (discriminator 4)) __mld_query_work (net/ipv6/mcast.c:1495) (discriminator 1)) mld_query_work (net/ipv6/mcast.c:1563) process_one_work (kernel/workqueue.c:3314) worker_thread (kernel/workqueue.c:3397 kernel/workqueue.c:3478) kthread (kernel/kthread.c:436) ret_from_fork (arch/x86/kernel/process.c:158) ret_from_fork_asm (arch/x86/entry/entry_64.S:245)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Take the SRCU lock for page table walks in fault injection and AT emulation walk_s1() and kvm_walk_nested_s2() expect to be called while holding kvm->srcu to guard against memslot changes. While this is generally the case, __kvm_at_s12() and __kvm_find_s1_desc_level() call into the respective walkers without taking kvm->srcu. Fix by acquiring kvm->srcu prior to the table walk in both instances.	2026-06-25	8.8	CVE-2026-53277
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Avoid NULL pointer dereference or refcount corruption Commit 60f030f7418d ("iommu/vt-d: Avoid use of NULL after WARN_ON_ONCE") fixed a NULL pointer dereference in an unlikely situation partly. If dev_pasid is not found in the dev_pasids list, it remains NULL. However, the teardown operations are executed unconditionally, this lead to a NULL pointer dereference or refcount corruption. If the domain was never attached to this IOMMU, info will be NULL, which would cause an immediate dereference when checking --info->refcnt. Even if info is not NULL, decrementing the refcount without having removed a valid PASID might unbalance the count. This could lead to premature dropping of the refcount to 0, potentially causing a use-after-free for the remaining active devices sharing the domain. Fix it by returning early if dev_pasid is NULL, before executing the teardown operations. Issue found by AI review and suggested by Kevin Tian. https://sashiko.dev/#/patchset/20260421031347.1408890-1-zhenzhong.duan%40intel.com	2026-06-26	8.8	CVE-2026-53281
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vfio/pci: Clean up DMABUFs before disabling function On device shutdown, make vfio_pci_core_close_device() call vfio_pci_dma_buf_cleanup() before the function is disabled via vfio_pci_core_disable(). This ensures that all access via DMABUFs is revoked before the function's BARs become inaccessible. This fixes an issue where, if the function is disabled first, a tiny window exists in which the function's MSE is cleared and yet BARs could still be accessed via the DMABUF. The resources would also be freed and up for grabs by a different driver.	2026-06-26	8.8	CVE-2026-53322
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_queue: hold bridge skb->dev while queued br_pass_frame_up() rewrites skb->dev from the ingress port to the bridge master before queueing bridge LOCAL_IN packets. NFQUEUE only holds references on state.in/out and bridge physdevs, so a queued bridge packet can retain a freed bridge master in skb->dev until reinjection. When the verdict is reinjected later, br_netif_receive_skb() re-enters the receive path with skb->dev still pointing at the freed bridge master, triggering a use-after-free. Store skb->dev in the queue entry, hold a reference on it for the queue lifetime, and use the saved device when dropping queued packets during NETDEV_DOWN handling.	2026-06-24	7.8	CVE-2026-52912
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: ip6t_hbh: reject oversized option lists struct ip6t_opts stores at most IP6T_OPTS_OPTSNR option descriptors, but hbh_mt6_check() does not	2026-06-24	7.1	CVE-2026-52915

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	reject larger optsnr values supplied from userspace. Validate optsnr in the rule setup path so only match data that fits the fixed-size opts array can be installed. This follows the existing xtables pattern of rejecting invalid user-provided counts in checkentry() and keeps the packet matching path unchanged. `struct ip6t_opts` has a fixed `opts[IP6T_OPTS_OPTSNR]` array, where `IP6T_OPTS_OPTSNR` is 16, then off-by-one array access is possible: [137.924693][T8692] UBSAN: array-index-out-of-bounds in ../net/ipv6/netfilter/ip6t_hbh.c:110:29 [137.926167][T8692] index 16 is out of range for type ' __u16 [16]'			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: diag: reject stale associations in dump_one path The SCTP exact sock_diag lookup can hold a transport reference, block on lock_sock(sk), and then resume after sctp_association_free() has marked the association dead and freed its bind address list. When that happens, inet_assoc_attr_size() and inet_diag_msg_sctpasoc_fill() can still dereference association state that is no longer valid for reporting. In particular, inet_diag_msg_sctpasoc_fill() may read an empty bind-address list as a real sctp_sockaddr_entry and trigger an out-of-bounds read from unrelated association memory. Reject the association after taking the socket lock if it has been reaped or detached from the endpoint, and report the lookup as stale. This keeps the exact dump-one path from formatting torn association state.	2026-06-24	7.1	CVE-2026-52917
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: fix tp_meter counter underflow during shutdown batadv_tp_sender_shutdown() unconditionally decrements the "sending" atomic counter. If multiple paths (e.g. timeout, user cancel, and normal finish) call this function, the counter can underflow to -1. Since the sender logic treats any non-zero value as "still sending", a negative value causes the sender kthread to loop indefinitely. This leads to a use-after-free when the interface is removed while the zombie thread is still active. Fix this by using atomic_xchg() to ensure the counter only transitions from 1 to 0 once. [sven: added missing change in batadv_tp_send]	2026-06-24	7.8	CVE-2026-52919
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: batman-adv: dat: handle forward allocation error batadv_dat_forward_data() calls pskb_copy_for_clone() to duplicate an skb for each DHT candidate, but does not check the return value before passing it to batadv_send_skb_prepare_unicast_4addr(). That function dereferences the skb unconditionally, so a failed allocation triggers a NULL pointer dereference. Skip forwarding to the current DHT candidate on allocation failure.	2026-06-24	7.5	CVE-2026-52922
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipc: limit next_id allocation to the valid ID range The checkpoint/restore sysctl path can request the next SysV IPC id through ids->next_id. ipc_idr_alloc() currently forwards that request to idr_alloc() with an open-ended upper bound. If the valid tail of the SysV IPC id space is full, the allocation can spill beyond ipc_mni. The returned SysV IPC id still uses the normal index encoding, so later lookup and removal can target the wrong slot. This leaves the real IDR entry behind and breaks the IDR state for the object. The bug is in ipc_idr_alloc() in the checkpoint/restore path. 1. ids->next_id is passed to: idr_alloc(&ids->ipcs_idr, new, ipcid_to_idx(next_id), 0, ...) 2. The zero upper bound makes the allocation effectively open-ended. Once the valid SysV IPC tail is occupied, idr_alloc() can spill past ipc_mni and allocate an entry beyond the valid IPC id range. 3. The new object id is still encoded with the narrower SysV IPC index width: new->id = (new->seq << ipcmni_seq_shift()) + idx 4. Later removal goes through ipc_rmid(), which uses: ipcid_to_idx(ipcp->id) That truncates the real IDR index. An object actually stored at a high index can then be removed as if it lived at a low in-range index. 5. For shared memory, shm_destroy() frees the current object anyway, but the real high IDR slot is left behind as a dangling pointer. 6. A subsequent walk of /proc/sysvipc/shm reaches the stale IDR	2026-06-24	7.8	CVE-2026-52923

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	entry and dereferences freed memory. Prevent this by bounding the requested allocation to ipc_mni so the checkpoint/restore path fails once the valid range is exhausted.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: ebtables: fix OOB read in compat_mtw_from_user Luxiao Xu says: The function compat_mtw_from_user() converts ebtables extensions from 32-bit user structures to kernel native structures. However, it lacks proper validation of the user-supplied match_size/target_size. When certain extensions are processed, the kernel-side translation logic may perform memory accesses based on the extension's expected size. If the user provides a size smaller than what the extension requires, it results in an out-of-bounds read as reported by KASAN. This fix introduces a check to ensure match_size is at least as large as the extension's required compatsize. This covers matches, watchers, and targets, while maintaining compatibility with standard targets. AFAIU this is relevant for matches that need to go through match->compat_from_user() call. Those that use plain memcpy with the user-provided size are ok because the caller checks that size vs the start of the next rule entry offset (which itself is checked vs. total size copied from userspace). The ->compat_from_user() callbacks assume they can read compatsize bytes, so they need this extra check. Based on an earlier patch from Luxiao Xu.	2026-06-24	7.8	CVE-2026-52927
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: stream: fully roll back denied add-stream state When ADD_OUT_STREAMS is denied, SCTP only shrinks the queued chunks and then lowers outcnt. That leaves removed stream metadata behind, so a later re-add can reuse a stale ext and hit a null-pointer dereference in the scheduler get path. Fix the rollback by tearing down the removed stream state the same way other stream resizes do. Unschedule the current scheduler state, drop the removed stream ext state with sctp_stream_outq_migrate(), and then reschedule the remaining streams. This keeps scheduler-private RR/FC/PRIOR lists consistent while fully rolling back denied outgoing stream additions.	2026-06-24	7.5	CVE-2026-52929
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: ipcomp: Free destination pages on acomp errors Move the out_free_req label up by a couple of lines so that the allocated dst SG list gets freed on error as well as success.	2026-06-24	7.5	CVE-2026-52932
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: io_uring/poll: fix signed comparison in io_poll_get_ownership() io_poll_get_ownership() uses a signed comparison to check whether poll_refs has reached the threshold for the slowpath: if (unlikely(atomic_read(&req->poll_refs) >= IO_POLL_REF_BIAS)) atomic_read() returns int (signed). When IO_POLL_CANCEL_FLAG (BIT(31)) is set in poll_refs, the value becomes negative in signed arithmetic, so the >= 128 comparison always evaluates to false and the slowpath is never taken. Fix this by casting the atomic_read() result to unsigned int before the comparison, so that the cancel flag is treated as a large positive value and correctly triggers the slowpath.	2026-06-24	7.8	CVE-2026-52933
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: espintcp: do not reuse an in-progress partial send espintcp keeps a single in-flight transmit in ctx->partial. Before building a new sk_msg, espintcp_sendmsg() first tries to flush that state through espintcp_push_msgs(). For blocking callers, espintcp_push_msgs() may return success even when the previous partial send is still pending. espintcp_sendmsg() would then reinitialize msg->skmsg and reuse ctx->partial while the old transfer still owns that state. Do not rebuild the send message when ctx->partial is still in progress. If espintcp_push_msgs() returns with msg->len still set, fail the new send instead of overwriting the live partial state. This is a memory-safety fix: reusing the live partial-send state can leave a stale offset attached to a new sk_msg and lead to	2026-06-24	7.8	CVE-2026-52935

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	an out-of- bounds read in the send path. tcp_sendmsg_locked() already handles waiting for send buffer memory, so the fix here is just to preserve espintcp's one-message-at-a-time transmit state.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_log: validate MAC header was set before dumping it The fallback path of dump_mac_header() guards the MAC header access only with "skb->mac_header != skb->network_header", without checking skb_mac_header_was_set(). When the MAC header is unset, mac_header is 0xffff, so the test passes and skb_mac_header(skb) returns skb->head + 0xffff, ~64 KiB past the buffer; the loop then reads dev->hard_header_len bytes out of bounds into the kernel log. This is reachable via the netdev logger: nf_log_unknown_packet() calls dump_mac_header() unconditionally, and an skb sent through AF_PACKET with PACKET_QDISC_BYPASS reaches the egress hook with mac_header still unset (__dev_queue_xmit(), which would reset it, is bypassed). Add the skb_mac_header_was_set() check the ARPDRD_ETHER path already uses, and replace the open-coded MAC header length test with skb_mac_header_len(). Only skbs with an unset MAC header are affected; valid ones are dumped as before. BUG: KASAN: slab-out-of-bounds in dump_mac_header (net/netfilter/nf_log_syslog.c:831) Read of size 1 at addr ffff88800ea49d3f by task exploit/148 Call Trace: kasan_report (mm/kasan/report.c:595) dump_mac_header (net/netfilter/nf_log_syslog.c:831) nf_log_netdev_packet (net/netfilter/nf_log_syslog.c:938 net/netfilter/nf_log_syslog.c:963) nf_log_packet (net/netfilter/nf_log.c:260) nft_log_eval (net/netfilter/nft_log.c:60) nft_do_chain (net/netfilter/nf_tables_core.c:285) nft_do_chain_netdev (net/netfilter/nft_chain_filter.c:307) nf_hook_slow (net/netfilter/core.c:619) nf_hook_direct_egress (net/packet/af_packet.c:257) packet_xmit (net/packet/af_packet.c:280) packet_sendmsg (net/packet/af_packet.c:3114) __sys_sendto (net/socket.c:2265)	2026-06-24	7.1	CVE-2026-52942
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: skbuff: fix missing zerocopy reference in pskb_carve helpers pskb_carve_inside_header() and pskb_carve_inside_nonlinear() both copy the old skb_shared_info header into a new buffer via memcpy(), which includes the destructor_arg pointer (uarg) for MSG_ZEROCOPY skbs. Neither function calls net_zcopy_get() for the new shinfo, creating an unaccounted holder: every skb_shared_info with destructor_arg set will call skb_zcopy_clear() once when freed, but the corresponding net_zcopy_get() was never called for the new copy. Repeated calls drive uarg->refcnt to zero prematurely, freeing ubuf_info_msgz while TX skbs still hold live destructor_arg pointers. KASAN reports use-after-free on a freed ubuf_info_msgz: BUG: KASAN: slab-use-after-free in skb_release_data+0x77b/0x810 Read of size 8 at addr ffff88801574d3e8 by task poc/220 Call Trace: skb_release_data+0x77b/0x810 kfree_skb_list_reason+0x13e/0x610 skb_release_data+0x4cd/0x810 sk_skb_reason_drop+0xf3/0x340 skb_queue_purge_reason+0x282/0x440 rds_tcp_inc_free+0x1e/0x30 rds_rcvmsg+0x354/0x1780 __sys_rcvmsg+0xdf/0x180 Allocated by task 219: msg_zerocopy_realloc+0x157/0x7b0 tcp_sendmsg_locked+0x2892/0x3ba0 Freed by task 219: ip_rcv_error+0x74a/0xb10 tcp_rcvmsg+0x475/0x530 The skb consuming the late access still referenced the same uarg via shinfo->destructor_arg copied by pskb_carve_inside_nonlinear() without a refcount bump. This has been verified to be reliably exploitable: a working proof-of-concept achieves full root privilege escalation from an unprivileged local user on a default kernel configuration. The fix follows the pattern of pskb_expand_head() which has the same memcpy/cloned structure. For pskb_carve_inside_header(), net_zcopy_get() is placed after	2026-06-24	7.8	CVE-2026-52943

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	skb_orphan_frags() succeeds, so the orphan error path needs no cleanup. For pskb_carve_inside_nonlinear(), net_zcopy_get() is placed after all failure points and just before skb_release_data(), so no error path needs cleanup at all -- matching pskb_expand_head() more closely and avoiding the need for a balancing net_zcopy_put().			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Revert "wireguard: device: enable threaded NAPI" This reverts commit 933466fc50a8e4eb167acbd0d8ec96a078462e9c which is commit db9ae3b6b43c79b1ba87eea849fd65efa05b4b2e upstream. We have had three independent production user reports in combination with Cilium utilizing WireGuard as encryption underneath that k8s Pod E/W traffic to certain peer nodes fully stalled. The situation appears as follows: - Occurs very rarely but at random times under heavy networking load. - Once the issue triggers the decryption side stops working completely for that WireGuard peer, other peers keep working fine. The stall happens also for newly initiated connections towards that particular WireGuard peer. - Only the decryption side is affected, never the encryption side. - Once it triggers, it never recovers and remains in this state, the CPU/mem on that node looks normal, no leak, busy loop or crash. - bpftrace on the affected system shows that wg_prev_queue_enqueue fails, thus the MAX_QUEUED_PACKETS (1024 skbs!) for the peer's rx_queue is reached. - Also, bpftrace shows that wg_packet_rx_poll for that peer is never called again after reaching this state for that peer. For other peers wg_packet_rx_poll does get called normally. - Commit db9ae3b ("wireguard: device: enable threaded NAPI") switched WireGuard to threaded NAPI by default. The default has not been changed for triggering the issue, neither did CPU hotplugging occur (i.e. 5bd8de2 ("wireguard: queueing: always return valid online CPU in wg_cpumask_choose_online()")). - The issue has been observed with stable kernels of v5.15 as well as v6.1. It was reported to us that v5.10 stable is working fine, and no report on v6.6 stable either (somewhat related discussion in [0] though). - In the WireGuard driver the only material difference between v5.10 stable and v5.15 stable is the switch to threaded NAPI by default. [0] https://lore.kernel.org/netdev/CA+wXwBTT74RErDGAnj98PqS=wvdh8eM1pi4q6tTdExtjnokKqA@mail.gmail.com/ Breakdown of the problem: 1) skbs arriving for decryption are enqueued to the peer->rx_queue in wg_packet_consume_data via wg_queue_enqueue_per_device_and_peer. 2) The latter only moves the skb into the MPSC peer queue if it does not surpass MAX_QUEUED_PACKETS (1024) which is kept track in an atomic counter via wg_prev_queue_enqueue. 3) In case enqueueing was successful, the skb is also queued up in the device queue, round-robin picks a next online CPU, and schedules the decryption worker. 4) The wg_packet_decrypt_worker, once scheduled, picks these up from the queue, decrypts the packets and once done calls into wg_queue_enqueue_per_peer_rx. 5) The latter updates the state to PACKET_STATE_CRYPTED on success and calls napi_schedule on the per peer->napi instance. 6) NAPI then polls via wg_packet_rx_poll. wg_prev_queue_peek checks on the peer->rx_queue. It will wg_prev_queue_dequeue if the queue->peeked skb was not cached yet, or just return the latter otherwise. (wg_prev_queue_drop_peeked later clears the cache.) 7) From an ordering perspective, the peer->rx_queue has skbs in order while the device queue with the per-CPU worker threads from a global ordering PoV can finish the decryption and signal the skb PACKET_STATE_CRYPTED out of order. 8) A situation can be observed that the first packet coming in will be stuck waiting for the decryption worker to be scheduled for a longer time when the system is under pressure. 9) While this is the case, the other CPUs in the meantime finish decryption and call into napi_schedule. 10) Now in wg_packet_rx_poll it picks up the	2026-06-24	7.5	CVE-2026-52945

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	first in-order skb from the peer->rx_queue and sees that its state is still PACKET_STATE_UNCRYPTED. The NAPI poll routine then exits e --- truncated---			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fs/fcntl: fix SOFTIRQ-unsafe lock order in fasync signaling A SOFTIRQ-safe to SOFTIRQ-unsafe lock order deadlock can occur in send_sigio() and send_sigurg() when a process group receives a signal. When FASYNC is configured for a process group (PIDTYPE_PGID), both functions use read_lock(&tasklist_lock) to traverse the task list. However, they are frequently called from softirq context: - send_sigio() via input_inject_event -> kill_fasync - send_sigurg() via tcp_check_urg -> sk_send_sigurg (NET_RX_SOFTIRQ) The deadlock is caused by the rwlock writer fairness mechanism: 1. CPU 0 (process context) holds read_lock(&tasklist_lock) in do_wait(). 2. CPU 1 (process context) attempts write_lock(&tasklist_lock) in fork() or exit() and spins, which blocks all new readers. 3. CPU 0 is interrupted by a softirq (e.g., TCP URG packet reception). 4. The softirq calls send_sigurg() and attempts to acquire read_lock(&tasklist_lock), deadlocking because CPU 1 is waiting. Since PID hashing and do_each_pid_task() traversals are already RCU-protected, the read_lock on tasklist_lock is no longer strictly required for safe traversal. Fix this by replacing tasklist_lock with rcu_read_lock(), aligning the process group signaling path with the single-PID path. This also mitigates a potential remote denial of service vector via TCP URG packets. Lockdep splat: ===== WARNING: SOFTIRQ-safe -> SOFTIRQ-unsafe lock order detected [...] Chain exists of: &dev->event_lock --> &f_owner->lock --> tasklist_lock Possible interrupt unsafe locking scenario: CPU0 CPU1 ---- ---- lock(tasklist_lock); local_irq_disable(); lock(&dev->event_lock); lock(&f_owner->lock); <Interrupt> lock(&dev->event_lock); *** DEADLOCK ***	2026-06-24	7.5	CVE-2026-52946
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: qrtr: fix refcount saturation and potential UAF in qrtr_port_remove In qrtr_port_remove(), the socket reference count is decremented via __sock_put() before the port is removed from the qrtr_ports XArray and before the RCU grace period elapses. This breaks the fundamental RCU update paradigm. It exposes a race window where a concurrent RCU reader (such as qrtr_reset_ports() or qrtr_port_lookup()) can obtain a pointer to the socket from the XArray, and attempt to call sock_hold() on a socket whose reference count has already dropped to zero. This exact race condition was hit during syzkaller fuzzing, leading to the following refcount saturation warning and a potential Use-After-Free: refcount_t: saturated; leaking memory. WARNING: CPU: 3 PID: 1273 at lib/refcount.c:22 refcount_warn_saturate+0xae/0x1d0 Modules linked in: qrtr(+) bochs drm_shmem_helper ... Call Trace: <TASK> qrtr_reset_ports net/qrtr/af_qrtr.c:768 [inline] [qrtr] __qrtr_bind.isra.0+0x48b/0x570 net/qrtr/af_qrtr.c:805 [qrtr] qrtr_bind+0x17d/0x210 net/qrtr/af_qrtr.c:901 [qrtr] kernel_bind+0xe4/0x120 net/socket.c:3592 qrtr_ns_init+0x1a6/0x380 net/qrtr/ns.c:715 [qrtr] qrtr_proto_init+0x3b/0xff0 net/qrtr/af_qrtr.c:169 [qrtr] do_one_initcall+0xf5/0x5e0 init/main.c:1283 ... </TASK> Fix this by deferring the reference count decrement until after the xa_erase() and the synchronize_rcu() complete. (Note: The v1 of this patch incorrectly replaced __sock_put() with sock_put(). As Simon Horman pointed out, the callers of qrtr_port_remove() still hold a reference to the socket, so freeing the socket memory here would lead to a subsequent UAF in the caller. Thus, the __sock_put() is kept, but only repositioned to close the RCU race.)	2026-06-24	7.8	CVE-2026-52947
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/dma-buf: fix UAF with retry loop Retry doesn't work here, since bo will be freed on error, leading to UAF. However, now that we do the alloc	2026-06-24	7.8	CVE-2026-52950

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	& init before the attach, we can now combine this as one unit and have the init do the alloc for us. This should make the retry safe. Reported by Sashiko. v2: Fix up the error unwind (CI) (cherry picked from commit 479669418253e0f27f8cf5db01a731352ea592e7)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/dma-buf: handle empty bo and UAF races There look to be some nasty races here when triggering the invalidate_mappings hook: 1) We do xe_bo_alloc() followed by the attach, before the actual full bo init step in xe_dma_buf_init_obj(). However the bo is visible on the attachments list after the attach. This is bad since exporter driver, say amdgpu, can at any time call back into our invalidate_mappings hook, with an empty/bogus bo, leading to potential bugs/crashes. 2) Similar to 1) but here we get a UAF, when the invalidate_mappings hook is triggered. For example, we get as far as xe_bo_init_locked() but this fails in some way. But here the bo will be freed on error, but we still have it attached from dma-buf pov, so if the invalidate_mappings is now triggered then the bo we access is gone and we trigger UAF and more bugs/crashes. To fix this, move the attach step until after we actually have a fully set up buffer object. Note that the bo is not published to userspace until later, so not sure what the comment "Don't publish the bo until we have a valid attachment", is referring to. We have at least two different customers reporting hitting a NULL ptr deref in evict_flags when importing something from amdgpu, followed by triggering the evict flow. Hit rate is also pretty low, which would hint at some kind of race, so something like 1) or 2) might explain this. v2: - Shuffle the order of the ops slightly (no functional change) - Improve the comment to better explain the ordering (Matt B) (cherry picked from commit af1f2ad0c59fe4e2f924c526f66e968289d77971)	2026-06-24	7.8	CVE-2026-52951
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Fix oops due to out of scope access Below oops triggers when kill QEMU process: Oops: general protection fault, probably for non-canonical address 0x7fffffff844eaaa7: 0000 [#1] SMP NOPTI Call Trace: <TASK> do_raw_spin_lock+0xaa/0xc0 _raw_spin_lock_irqsave+0x21/0x40 domain_remove_dev_pasid+0x52/0x160 intel_nested_set_dev_pasid+0x1b9/0x1e0 __iommu_set_group_pasid+0x56/0x120 pci_dev_reset_iommu_done+0xe3/0x180 pcie_flr+0x65/0x160 __pci_reset_function_locked+0x5b/0x120 vfio_pci_core_close_device+0x63/0xe0 [vfio_pci_core] vfio_df_close+0x4f/0xa0 vfio_df_unbind_iommufd+0x2d/0x60 vfio_device_fops_release+0x3e/0x40 __fput+0xe5/0x2c0 task_work_run+0x58/0xa0 do_exit+0x2c8/0x600 do_group_exit+0x2f/0xa0 get_signal+0x863/0x8c0 arch_do_signal_or_restart+0x24/0x100 exit_to_user_mode_loop+0x87/0x380 do_syscall_64+0x2ff/0x11e0 entry_SYSCALL_64_after_hwframe+0x76/0x7e The global static blocked domain is a dummy domain without corresponding dmar_domain structure, accessing beyond iommu_domain structure triggers oops easily. Fix it by return early in domain_remove_dev_pasid() like identity domain.	2026-06-24	7.1	CVE-2026-52953
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: handle rbtree insertion error in decode_choose_args() A message of type CEPH_MSG_OSD_MAP contains an OSD map that itself contains a CRUSH map. The received CRUSH map may optionally contain choose_args that get decoded in decode_choose_args(). In this function, num_choose_arg_maps is read from the message, and a corresponding number of crush_choose_arg_maps gets decoded afterwards. Each crush_choose_arg_map has a choose_args_index, which serves as the key when inserting it into the choose_args rbtree of the decoded crush_map. If a (potentially corrupted) message contains two crush_choose_arg_maps with the same index, the assertion in insert_choose_arg_map() triggers a	2026-06-24	7.5	CVE-2026-52954

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	kernel BUG when trying to insert the second crush_choose_arg_map. This patch fixes the issue by switching to the non-asserting rbtree insertion function and rejecting the message if the insertion fails. [idryomov: changelog]			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: Fix potential out-of-bounds access in __ceph_x_decrypt() In __ceph_x_decrypt(), a part of the buffer p is interpreted as a ceph_x_encrypt_header, and the magic field of this struct is accessed. This happens without any guarantee that the buffer is large enough to hold this struct. The function parameter ciphertxt_len represents the length of the ciphertxt to decrypt and is guaranteed to be at most the remaining size of the allocated buffer p. However, this value is not necessarily greater than sizeof(ceph_x_encrypt_header). E.g., a message frame of type FRAME_TAG_AUTH_REPLY_MORE, that is just as long to hold the ciphertxt at its end with a ciphertxt_len of 8 or less, can trigger an out-of-bounds memory access when accessing hdr->magic. This patch fixes the issue by adding a check to ensure that the decrypted plaintext in the buffer is large enough to represent at least the ceph_x_encrypt_header.	2026-06-24	7.5	CVE-2026-52956
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: libceph: Fix potential null-ptr-deref in decode_choose_args() A message of type CEPH_MSG_OSD_MAP contains an OSD map that itself contains a CRUSH map. When decoding this CRUSH map in crush_decode(), an array of max_buckets CRUSH buckets is decoded, where some indices may not refer to actual buckets and are therefore set to NULL. The received CRUSH map may optionally contain choose_args that get decoded in decode_choose_args(). When decoding a crush_choose_arg_map, a series of choose_args for different buckets is decoded, with the bucket_index being read from the incoming message. It is only checked that the bucket index does not exceed max_buckets, but not that it doesn't point to an index with a NULL bucket. If a (potentially corrupted) message contains a crush_choose_arg_map including such a bucket_index, a null pointer dereference may occur in the subsequent processing when attempting to access the bucket with the given index. This patch fixes the issue by extending the affected check. Now, it is only attempted to access the bucket if it is not NULL.	2026-06-24	7.5	CVE-2026-52957
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: virt: sev-guest: Do not use host-controlled page order in cleanup path When issuing an extended guest request (SVM_VMGEXIT_EXT_GUEST_REQUEST), get_ext_report() allocates a buffer to retrieve a certificate blob from the host, keeping track of its size in report_req->certs_len. However, the host may return SNP_GUEST_VMM_ERR_INVALID_LEN, indicating an invalid buffer size, as well as the expected length of such buffer. get_ext_report() subsequently updates report_req->certs_len with the host-controlled value, and cleans up the buffer by computing a page order from such value. This is incorrect, as the host-provided length may not match the page order of the original allocation, potentially resulting in corruption in the page allocator. Fix this by using alloc_pages_exact() instead, and reusing @npages to compute the size passed to free_pages_exact(). For consistency, also use @npages to compute the size when allocating the pages, even though this last change has no functional effect.	2026-06-24	7.8	CVE-2026-52959
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ceph: put folios not suitable for writeback The batch holds references to the folios (see `filemap_get_folios`, `folio_batch_release`), so we need to `folio_put` the folios we remove. Tested on v6.18.	2026-06-24	7.5	CVE-2026-52960
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: ena: PHC: Fix potential use-after-free in get_timestamp Move the phc->active check and resp pointer assignment to after acquiring the spinlock. Previously, phc->active was checked without holding the lock, and resp was cached from ena_dev->phc.virt_addr before the lock was acquired. If	2026-06-24	7.8	CVE-2026-52971

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ena_com_phc_destroy() runs between the lockless active check and the lock acquisition, it sets active=false, releases the lock, frees the DMA memory, and sets virt_addr=NULL. The get_timestamp path would then read a NULL virt_addr and dereference it. With both the active check and the pointer read under the lock, destroy cannot free the memory while get_timestamp is using it.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: futex: Drop CLONE_THREAD requirement for private default hash alloc Currently need_futex_hash_allocate_default() depends on strict pthread semantics, abusing CLONE_THREAD. This breaks the non-concurrency assumptions when doing the mm->futex_ref pcpu allocations, leading to bugs[0] when sharing the mm in other ways; ie: BUG: KASAN: slab-use-after-free in futex_hash_put ... where the +1 bias can end up on a percpu counter that mm->futex_ref no longer points at. Loosen the check to cover any CLONE_VM clone, except vfork(). Excluding vfork keeps the existing paths untouched (no overhead), and we can't race in the first place: either the parent is suspended and the child runs alone, or mm->futex_ref is already allocated from an earlier CLONE_VM.	2026-06-24	7.8	CVE-2026-52973
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: tls: fix strparser anchor skb leak on offload RX setup failure When tls_set_device_offload_rx() fails at tls_dev_add(), the error path calls tls_sw_free_resources_rx() to clean up the SW context that was initialized by tls_set_sw_offload(). This function calls tls_sw_release_resources_rx() (which stops the strparser via tls_strp_stop()) and tls_sw_free_ctx_rx() (which kfree's the context), but never frees the anchor skb that was allocated by alloc_skb(0) in tls_strp_init(). Note that tls_sw_free_resources_rx() is exclusively used for this "failed to start offload" code path, there's no other caller. The leak did not exist before commit 84c61fe1a75b ("tls: rx: do not use the standard strparser"), because the standard strparser doesn't try to pre-allocate an skb. The normal close path in tls_sk_proto_close() handles cleanup by calling tls_sw_strparser_done() (which calls tls_strp_done()) after dropping the socket lock, because tls_strp_done() does cancel_work_sync() and the strparser work handler takes the socket lock.	2026-06-24	7.5	CVE-2026-52974
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bonding: 3ad: implement proper RCU rules for port->aggregator syzbot found a data-race in bond_3ad_get_active_agg_info / bond_3ad_state_machine_handler [1] which hints at lack of proper RCU implementation. Add __rcu qualifier to port->aggregator, and add proper RCU API. [1] BUG: KCSAN: data-race in bond_3ad_get_active_agg_info / bond_3ad_state_machine_handler write to 0xffff88813cf5c4b0 of 8 bytes by task 36 on cpu 0: ad_port_selection_logic drivers/net/bonding/bond_3ad.c:1659 [inline] bond_3ad_state_machine_handler+0x9d5/0x2d60 drivers/net/bonding/bond_3ad.c:2569 process_one_work kernel/workqueue.c:3302 [inline] process_scheduled_works+0x4f0/0x9c0 kernel/workqueue.c:3385 worker_thread+0x58a/0x780 kernel/workqueue.c:3466 kthread+0x22a/0x280 kernel/kthread.c:436 ret_from_fork+0x146/0x330 arch/x86/kernel/process.c:158 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:245 read to 0xffff88813cf5c4b0 of 8 bytes by task 22063 on cpu 1: __bond_3ad_get_active_agg_info drivers/net/bonding/bond_3ad.c:2858 [inline] bond_3ad_get_active_agg_info+0x8c/0x230 drivers/net/bonding/bond_3ad.c:2881 bond_fill_info+0xe0f/0x10f0 drivers/net/bonding/bond_netlink.c:853 rtnl_link_info_fill net/core/rtnetlink.c:906 [inline] rtnl_link_fill+0x1d7/0x4e0 net/core/rtnetlink.c:927 rtnl_fill_ifinfo+0xf8e/0x1380 net/core/rtnetlink.c:2168 rtmsg_ifinfo_build_skb+0x11c/0x1b0 net/core/rtnetlink.c:4453 rtmsg_ifinfo_event net/core/rtnetlink.c:4486	2026-06-24	7.8	CVE-2026-52975

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	[inline] rtmsg_ifinfo+0x6d/0x110 net/core/rtnetlink.c:4495 __dev_notify_flags+0x76/0x390 net/core/dev.c:9790 netif_change_flags+0xac/0xd0 net/core/dev.c:9823 do_setlink+0x905/0x2950 net/core/rtnetlink.c:3180 rtnl_group_changelink net/core/rtnetlink.c:3813 [inline] __rtnl_newlink net/core/rtnetlink.c:3981 [inline] rtnl_newlink+0xf55/0x1400 net/core/rtnetlink.c:4109 rtnetlink_rcv_msg+0x64b/0x720 net/core/rtnetlink.c:6995 netlink_rcv_skb+0x123/0x220 net/netlink/af_netlink.c:2550 rtnetlink_rcv+0x1c/0x30 net/core/rtnetlink.c:7022 netlink_unicast_kernel net/netlink/af_netlink.c:1318 [inline] netlink_unicast+0x5a8/0x680 net/netlink/af_netlink.c:1344 netlink_sendmsg+0x5c8/0x6f0 net/netlink/af_netlink.c:1894 sock_sendmsg_nosec net/socket.c:787 [inline] __sock_sendmsg net/socket.c:802 [inline] __sys_sendmsg+0x563/0x5b0 net/socket.c:2698 __sys_sendmsg+0x195/0x1e0 net/socket.c:2752 __sys_sendmsg net/socket.c:2784 [inline] __do_sys_sendmsg net/socket.c:2789 [inline] __se_sys_sendmsg net/socket.c:2787 [inline] __x64_sys_sendmsg+0xd4/0x160 net/socket.c:2787 x64_sys_call+0x194c/0x3020 arch/x86/include/generated/asm/syscalls_64.h:47 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0x12c/0x3b0 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0xf value changed: 0x0000000000000000 -> 0xffff88813cf5c400 Reported by Kernel Concurrency Sanitizer on: CPU: 1 UID: 0 PID: 22063 Comm: syz.0.31122 Tainted: G W syzkaller #0 PREEMPT(full) Tainted: [W]=WARN Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 04/18/2026			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix error cleanup in xe_exec_queue_create_ioctl() Two error handling issues exist in xe_exec_queue_create_ioctl(): 1. When xe_hw_engine_group_add_exec_queue() fails, the error path jumps to put_exec_queue which skips xe_exec_queue_kill(). If the VM is in preempt fence mode, xe_vm_add_compute_exec_queue() has already added the queue to the VM's compute exec queue list. Skipping the kill leaves the queue on that list, leading to a dangling pointer after the queue is freed. 2. When xa_alloc() fails after xe_hw_engine_group_add_exec_queue() has succeeded, the error path does not call xe_hw_engine_group_del_exec_queue() to remove the queue from the hw engine group list. The queue is then freed while still linked into the hw engine group, causing a use-after-free. Fix both by: - Changing the xe_hw_engine_group_add_exec_queue() failure path to jump to kill_exec_queue so that xe_exec_queue_kill() properly removes the queue from the VM's compute list. - Adding a del_hw_engine_group label before kill_exec_queue for the xa_alloc() failure path, which removes the queue from the hw engine group before proceeding with the rest of the cleanup. (cherry picked from commit 37c831f401746a45d510b312b0ed7a77b1e06ec8)	2026-06-24	7.8	CVE-2026-52976
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: neigh: let neigh_xmit take skb ownership neigh_xmit always releases the skb, except when no neighbour table is found. But even the first added user of neigh_xmit (mpls) relied on neigh_xmit to release the skb (or queue it for tx). sashiko reported: If neigh_xmit() is called with an uninitialized neighbor table (for example, NEIGH_ND_TABLE when IPv6 is disabled), it returns -EAFNOSUPPORT and bypasses its internal out_kfree_skb error path. Because the return value of neigh_xmit() is ignored here, does this leak the SKB? Assume full ownership and remove the last code path that doesn't xmit or free skb.	2026-06-24	7.5	CVE-2026-52981

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: airoha: fix BQL imbalance in TX path Fix a possible BQL imbalance in airoha_dev_xmit(), where inflight packets are accounted only for the AIROHA_NUM_TX_RING netdev TX queues. The queue index is computed as: qid = skb_get_queue_mapping(skb) % ARRAY_SIZE(qdma->q_tx) txq = netdev_get_tx_queue(dev, qid); However, airoha_qdma_tx_napi_poll() accounts completions across all netdev TX queues (num_tx_queues), leading to inconsistent BQL accounting. Also reset all netdev TX queues in the ndo_stop callback.	2026-06-24	7.5	CVE-2026-52983
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: avoid double drm_exec_fini() in userq validate When new_addition is true, amdgpu_userq_vm_validate() calls drm_exec_fini(&exec) before iterating over the collected HMM ranges and calling amdgpu_ttm_tt_get_user_pages(). If amdgpu_ttm_tt_get_user_pages() fails in that path, the code jumps to unlock_all and calls drm_exec_fini(&exec) a second time on the same exec object. drm_exec_fini() is not idempotent: it frees exec->objects and may also drop exec->contended and finalize the ww acquire context. Route that error path directly to the range cleanup once exec has already been finalized. Issue found using a prototype static analysis tool and confirmed by code review. (cherry picked from commit 2802952e4a07306da6ebe813ff1acacc5691851a)	2026-06-24	7.8	CVE-2026-52987
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: join hook list via splice_list_rcu() in commit phase Publish new hooks in the list into the basechain/flowtable using splice_list_rcu() to ensure netlink dump list traversal via rcu is safe while concurrent ruleset update is going on.	2026-06-24	7.1	CVE-2026-52988
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sched/psi: fix race between file release and pressure write A potential race condition exists between pressure write and cgroup file release regarding the priv member of struct kernfs_open_file, which triggers the uaf reported in [1]. Consider the following scenario involving execution on two separate CPUs: CPU0 CPU1 ===== vfs_rmdir() kernfs_iop_rmdir() cgroup_rmdir() cgroup_kn_lock_live() cgroup_destroy_locked() cgroup_addrm_files() cgroup_rm_file() kernfs_remove_by_name() kernfs_remove_by_name_ns() vfs_write() __kernfs_remove() new_sync_write() kernfs_drain() kernfs_fop_write_iter() kernfs_drain_open_files() cgroup_file_write() kernfs_release_file() pressure_write() cgroup_file_release() ctx = of->priv; kfree(ctx); of->priv = NULL; cgroup_kn_unlock() cgroup_kn_lock_live() cgroup_get(cgrp) cgroup_kn_unlock() if (ctx->psi.trigger) // here, trigger uaf for ctx, that is of->priv The cgroup_rmdir() is protected by the cgroup_mutex, it also safeguards the memory deallocation of of->priv performed within cgroup_file_release(). However, the operations involving of->priv executed within pressure_write() are not entirely covered by the protection of cgroup_mutex. Consequently, if the code in pressure_write(), specifically the section handling the ctx variable executes after cgroup_file_release() has completed, a uaf vulnerability involving of->priv is triggered. Therefore, the issue can be resolved by extending the scope of the cgroup_mutex lock within pressure_write() to encompass all code paths involving of->priv, thereby properly synchronizing the race condition occurring between cgroup_file_release() and pressure_write(). And, if an live kn lock can be successfully acquired while executing the pressure write operation, it indicates that the cgroup deletion process has not yet reached its final stage; consequently, the priv pointer within open_file cannot be NULL. Therefore, the operation to retrieve the ctx value must be moved to a point *after* the live kn lock has been successfully acquired. In another situation, specifically after entering cgroup_kn_lock_live() but before acquiring cgroup_mutex, there exists a different class of race	2026-06-24	7.8	CVE-2026-52991

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	condition: CPU0: write memory.pressure CPU1: write cgroup.pressure=0 ===== kernfs_fop_write_iter() kernfs_get_active_of(of) pressure_write() cgroup_kn_lock_live(memory.pressure) cgroup_tryget(cgrp) kernfs_break_active_protection(kn) ... blocks on cgroup_mutex cgroup_pressure_write() cgroup_kn_lock_live(cgroup.pressure) cgroup_file_show(memory.pressure, false) kernfs_show(false) kernfs_drain_open_files() cgroup_file_release(of) kfree(ctx) of->priv = NULL cgroup_kn_unlock() ... acquires cgroup_mutex ctx = of->priv; // may now be NULL if (ctx->psi.trigger) // NULL dereference Consequently, there is a possibility that of->priv is NULL, the pressure write needs to check for this. Now that the scope of the cgroup_mutex has been expanded, the original explicit cgroup_get/put operations are no longer necessary, this is because acquiring/releasing the live kn lock inherently executes a cgroup get/put operation. [1] BUG: KASAN: slab-use-after-free in pressure_write+0xa4/0x210 kernel/cgroup/cgroup.c:4011 Call Trace: pressure_write+0xa4/0x210 kernel/cgroup/cgroup.c:4011 cgroup_file_write+0x36f/0x790 kernel/cgroup/cgroup.c:43 ---truncated---			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nfnetlink_osf: fix potential NULL dereference in ttl check The nf_osf_ttl() function accessed skb->dev to perform a local interface address lookup without verifying that the device pointer was valid. Additionally, the implementation utilized an in_dev_for_each_ifa_rcu loop to match the packet source address against local interface addresses. It assumed that packets from the same subnet should not see a decrement on the initial TTL. A packet might appear it is from the same subnet but it actually isn't especially in modern environments with containers and virtual switching. Remove the device dereference and interface loop. Replace the logic with a switch statement that evaluates the TTL according to the ttl_check.	2026-06-24	7.5	CVE-2026-52998
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nat: use kfree_rcu to release ops Florian Westphal says: "Historically this is not an issue, even for normal base hooks: the data path doesn't use the original nf_hook_ops that are used to register the callbacks. However, in v5.14 I added the ability to dump the active netfilter hooks from userspace. This code will peek back into the nf_hook_ops that are available at the tail of the pointer-array blob used by the datapath. The nat hooks are special, because they are called indirectly from the central nat dispatcher hook. They are currently invisible to the nfnl hook dump subsystem though. But once that changes the nat ops structures have to be deferred too." Update nf_nat_register_fn() to deal with partial exposition of the hooks from error path which can be also an issue for nfnetlink_hook.	2026-06-24	7.8	CVE-2026-53000
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: pppoe: drop PFC frames RFC 2516 Section 7 states that Protocol Field Compression (PFC) is NOT RECOMMENDED for PPPoE. In practice, pppd does not support negotiating PFC for PPPoE sessions, and the current PPPoE driver assumes an uncompressed (2-byte) protocol field. However, the generic PPP layer function ppp_input() is not aware of the negotiation result, and still accepts PFC frames. If a peer with a broken implementation or an attacker sends a frame with a compressed (1-byte) protocol field, the subsequent PPP payload is shifted by one byte. This causes the network header to be 4-byte misaligned, which may trigger unaligned access exceptions on some architectures. To reduce the attack surface, drop PPPoE PFC frames. Introduce ppp_skb_is_compressed_proto() helper function to be used in both ppp_generic.c and pppoe.c to avoid open- coding.	2026-06-24	7.5	CVE-2026-53003
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: af_unix: Drop all SCM attributes for SOCKMAP. SOCKMAP can hide inflight fd from AF_UNIX GC. When a socket in SOCKMAP receives skb with inflight fd,	2026-06-24	7.8	CVE-2026-53005

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sk_psock_verdict_data_ready() looks up the mapped socket and enqueue skb to its psock->ingress_skb. Since neither the old nor the new GC can inspect the psock queue, the hidden skb leaks the inflight sockets. Note that this cannot be detected via kmemleak because inflight sockets are linked to a global list. In addition, SOCKMAP redirect breaks the Tarjan-based GC's assumption that unix_edge.successor is always alive, which is no longer true once skb is redirected, resulting in use-after-free below. [0] Moreover, SOCKMAP does not call scm_stat_del() properly, so unix_show_fdinfo() could report an incorrect fd count. sk_msg_recvmg() does not support any SCM attributes in the first place. Let's drop all SCM attributes before passing skb to the SOCKMAP layer. [0]: BUG: KASAN: slab-use-after-free in unix_del_edges (net/unix/garbage.c:118 net/unix/garbage.c:181 net/unix/garbage.c:251) Read of size 8 at addr ffff888125362670 by task kworker/56:1/496 CPU: 56 UID: 0 PID: 496 Comm: kworker/56:1 Not tainted 7.0.0-rc7-00263-gb9d8b856689d #3 PREEMPT(lazy) Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.17.0-debian-1.17.0-1 04/01/2014 Workqueue: events sk_psock_backlog Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:122) print_report (mm/kasan/report.c:379) kasan_report (mm/kasan/report.c:597) unix_del_edges (net/unix/garbage.c:118 net/unix/garbage.c:181 net/unix/garbage.c:251) unix_destroy_fpl (net/unix/garbage.c:317) unix_destruct_scm (./include/net/scm.h:80 ./include/net/scm.h:86 net/unix/af_unix.c:1976) sk_psock_backlog (./include/linux/skbuff.h:?) process_scheduled_works (kernel/workqueue.c:?) worker_thread (kernel/workqueue.c:?) kthread (kernel/kthread.c:438) ret_from_fork (arch/x86/kernel/process.c:164) ret_from_fork_asm (arch/x86/entry/entry_64.S:258) </TASK> Allocated by task 955: kasan_save_track (mm/kasan/common.c:58 mm/kasan/common.c:78) __kasan_slab_alloc (mm/kasan/common.c:369) kmem_cache_alloc_noprof (mm/slub.c:4539) sk_prot_alloc (net/core/sock.c:2240) sk_alloc (net/core/sock.c:2301) unix_create1 (net/unix/af_unix.c:1099) unix_create (net/unix/af_unix.c:1169) __sock_create (net/socket.c:1606) __sys_socketpair (net/socket.c:1811) __x64_sys_socketpair (net/socket.c:1863 net/socket.c:1860 net/socket.c:1860) do_syscall_64 (arch/x86/entry/syscall_64.c:?) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) Freed by task 496: kasan_save_track (mm/kasan/common.c:58 mm/kasan/common.c:78) kasan_save_free_info (mm/kasan/generic.c:587) __kasan_slab_free (mm/kasan/common.c:287) kmem_cache_free (mm/slub.c:6165) __sk_destruct (net/core/sock.c:2282 net/core/sock.c:2384) sk_psock_destroy (./include/net/sock.h:?) process_scheduled_works (kernel/workqueue.c:?) worker_thread (kernel/workqueue.c:?) kthread (kernel/kthread.c:438) ret_from_fork (arch/x86/kernel/process.c:164) ret_from_fork_asm (arch/x86/entry/entry_64.S:258)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ice: fix double-free of tx_buf skb If ice_tso() or ice_tx_csum() fail, the error path in ice_xmit_frame_ring() frees the skb, but the 'first' tx_buf still points to it and is marked as valid (ICE_TX_BUF_SKB). 'next_to_use' remains unchanged, so the potential problem will likely fix itself when the next packet is transmitted and the tx_buf gets overwritten. But if there is no next packet and the interface is brought down instead, ice_clean_tx_ring() -> ice_unmap_and_free_tx_buf() will find the tx_buf and free the skb for the second time. The fix is to reset the tx_buf type to ICE_TX_BUF_EMPTY in the error path, so that ice_unmap_and_free_tx_buf(). Move the initialization of 'first' up, to ensure it's already valid in case we hit the linearization error path. The bug was spotted by AI while I had it looking for something else. It also proposed an initial version of the patch. I reproduced the bug and tested the fix by adding code to inject failures, on	2026-06-24	7.8	CVE-2026-53009

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a build with KASAN. I looked for similar bugs in related Intel drivers and did not find any.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: taprio: fix use-after-free in advance_sched() on schedule switch In advance_sched(), when should_change_schedules() returns true, switch_schedules() is called to promote the admin schedule to oper. switch_schedules() queues the old oper schedule for RCU freeing via call_rcu(), but 'next' still points into an entry of the old oper schedule. The subsequent 'next->end_time = end_time' and rcu_assign_pointer(q->current_entry, next) are use-after-free. Fix this by selecting 'next' from the new oper schedule immediately after switch_schedules(), and using its pre-calculated end_time. setup_first_end_time() sets the first entry's end_time to base_time + interval when the schedule is installed, so the value is already correct. The deleted 'end_time = sched_base_time(admin)' assignment was also harmful independently: it would overwrite the new first entry's pre-calculated end_time with just base_time.	2026-06-24	7.8	CVE-2026-53011
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: ccp - copy IV using skcipher ivsize AF_ALG rfc3686-ctr-aes-ccp requests pass an 8-byte IV to the driver. ccp_aes_complete() restores AES_BLOCK_SIZE bytes into the caller's IV buffer while RFC3686 skciphers expose an 8-byte IV, so the restore overruns the provided buffer. Use crypto_skcipher_ivsize() to copy only the algorithm's IV length.	2026-06-24	7.8	CVE-2026-53016
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: um: Fix potential race condition in TLB sync During the TLB sync, we need to traverse and modify the page table, so we should hold the page table lock. Since full SMP support for threads within the same process is still missing, let's disable the split page table lock for simplicity.	2026-06-24	7.8	CVE-2026-53020
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: greybus: raw: fix use-after-free if write is called after disconnect If a user writes to the chardev after disconnect has been called, the kernel panics with the following trace (with CONFIG_INIT_ON_FREE_DEFAULT_ON=y): BUG: kernel NULL pointer dereference, address: 0000000000000218 ... Call Trace: <TASK> gb_operation_create_common+0x61/0x180 gb_operation_create_flags+0x28/0xa0 gb_operation_sync_timeout+0x6f/0x100 raw_write+0x7b/0xc7 [gb_raw] vfs_write+0xcf/0x420 ? task_mm_cid_work+0x136/0x220 ksys_write+0x63/0xe0 do_syscall_64+0xa4/0x290 entry_SYSCALL_64_after_hwframe+0x77/0x7f Disconnect calls gb_connection_destroy, which ends up freeing the connection object. When gb_operation_sync is called in the write file operations, its gets a freed connection as parameter and the kernel panics. The gb_connection_destroy cannot be moved out of the disconnect function, as the Greybus subsystem expect all connections belonging to a bundle to be destroyed when disconnect returns. To prevent this bug, use a rw lock to synchronize access between write and disconnect. This guarantees that the write function doesn't try to use a disconnected connection.	2026-06-24	7.8	CVE-2026-53024
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: greybus: raw: fix use-after-free on cdev close This addresses a use-after-free bug when a raw bundle is disconnected but its chardev is still opened by an application. When the application releases the cdev, it causes the following panic when init on free is enabled (CONFIG_INIT_ON_FREE_DEFAULT_ON=y): refcount_t: underflow; use-after-free. WARNING: CPU: 0 PID: 139 at lib/refcount.c:28 refcount_warn_saturate+0xd0/0x130 ... Call Trace: <TASK> cdev_put+0x18/0x30 __fput+0x255/0x2a0 __x64_sys_close+0x3d/0x80 do_syscall_64+0xa4/0x290 entry_SYSCALL_64_after_hwframe+0x77/0x7f The cdev is contained in the "gb_raw" structure, which is freed in the disconnect operation. When the cdev is released at a later time, cdev_put gets an address that points to freed memory. To fix this use-after-free,	2026-06-24	7.8	CVE-2026-53025

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	convert the struct device from a pointer to being embedded, that makes the lifetime of the cdev and of this device the same. Then, use cdev_device_add, which guarantees that the device won't be released until all references to the cdev have been released. Finally, delegate the freeing of the structure to the device release function, instead of freeing immediately in the disconnect callback.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: NFSD: fix nfs4_file access extra count in nfsd4_add_rdaccess_to_wrdeleg In nfsd4_add_rdaccess_to_wrdeleg, if fp->fi_fds[O_RDONLY] is already set by another thread, __nfs4_file_get_access should not be called to increment the nfs4_file access count since that was already done by the thread that added READ access to the file. The extra fi_access count in nfs4_file can prevent the corresponding nfsd_file from being freed. When stopping nfs-server service, these extra access counts trigger a BUG in kmem_cache_destroy() that shows nfsd_file object remaining on __kmem_cache_shutdown. This problem can be reproduced by running the Git project's test suite over NFS.	2026-06-24	7.5	CVE-2026-53026
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Validate node_id in arena_alloc_pages() arena_alloc_pages() accepts a plain int node_id and forwards it through the entire allocation chain without any bounds checking. Validate node_id before passing it down the allocation chain in arena_alloc_pages().	2026-06-24	7.8	CVE-2026-53031
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf, sockmap: Take state lock for af_unix iter When a BPF iterator program updates a sockmap, there is a race condition in unix_stream_bpf_update_proto() where the `peer` pointer can become stale[1] during a state transition TCP_ESTABLISHED -> TCP_CLOSE. CPU0 bpf CPU1 close ----- // unix_stream_bpf_update_proto() sk_pair = unix_peer(sk) if (unlikely(!sk_pair)) return -EINVAL; // unix_release_sock() skpair = unix_peer(sk); unix_peer(sk) = NULL; sock_put(skpair) sock_hold(sk_pair) // UaF More practically, this fix guarantees that the iterator program is consistently provided with a unix socket that remains stable during iterator execution. [1]: BUG: KASAN: slab-use-after-free in unix_stream_bpf_update_proto+0x155/0x490 Write of size 4 at addr ffff8881178c9a00 by task test_progs/2231 Call Trace: dump_stack_lvl+0x5d/0x80 print_report+0x170/0x4f3 kasan_report+0xe4/0x1c0 kasan_check_range+0x125/0x200 unix_stream_bpf_update_proto+0x155/0x490 sock_map_link+0x71c/0xec0 sock_map_update_common+0xbc/0x600 sock_map_update_elem+0x19a/0x1f0 bpf_prog_bbbf56096cdd4f01_selective_dump_unix+0x20c/0x217 bpf_iter_run_prog+0x21e/0xae0 bpf_iter_unix_seq_show+0x1e0/0x2a0 bpf_seq_read+0x42c/0x10d0 vfs_read+0x171/0xb20 ksys_read+0xff/0x200 do_syscall_64+0xf7/0x5e0 entry_SYSCALL_64_after_hwframe+0x76/0x7e Allocated by task 2236: kasan_save_stack+0x30/0x50 kasan_save_track+0x14/0x30 __kasan_slab_alloc+0x63/0x80 kmem_cache_alloc_noprof+0x1d5/0x680 sk_prot_alloc+0x59/0x210 sk_alloc+0x34/0x470 unix_create1+0x86/0x8a0 unix_stream_connect+0x318/0x15b0 __sys_connect+0xfd/0x130 __x64_sys_connect+0x72/0xd0 do_syscall_64+0xf7/0x5e0 entry_SYSCALL_64_after_hwframe+0x76/0x7e Freed by task 2236: kasan_save_stack+0x30/0x50 kasan_save_track+0x14/0x30 kasan_save_free_info+0x3b/0x70 __kasan_slab_free+0x47/0x70 kmem_cache_free+0x11c/0x590 __sk_destruct+0x432/0x6e0 unix_release_sock+0x9b3/0xf60 unix_release+0x8a/0xf0 __sock_release+0xb0/0x270 sock_close+0x18/0x20 __fput+0x36e/0xac0 fput_close_sync+0xe5/0x1a0 __x64_sys_close+0x7d/0xd0 do_syscall_64+0xf7/0x5e0 entry_SYSCALL_64_after_hwframe+0x76/0x7e	2026-06-24	7.8	CVE-2026-53033

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf, arm64: Fix off-by-one in check_imm signed range check check_imm(bits, imm): is used in the arm64 BPF JIT to verify that a branch displacement (in arm64 instruction units) fits into the signed N-bit immediate field of a B, B.cond or CBZ/CBNZ encoding before it is handed to the encoder. The macro currently tests for (imm > 0 && imm >> bits) (imm < 0 && ~imm >> bits) which admits values in [-2^N, 2^N) - effectively a signed (N+1)-bit range. A signed N-bit field only holds [-2^(N-1), 2^(N-1)), so the check admits one extra bit of range on each side. In particular, for check_imm19(), values in [2^18, 2^19) slip past the check but do not fit into the 19-bit signed imm19 field of B.cond. aarch64_insn_encode_immediate() then masks the raw value into the 19-bit field, setting bit 18 (the sign bit) and flipping a forward branch into a backward one. Same class of issue exists for check_imm26() and the B/BL encoding. Shift by (bits - 1) instead of bits so the actual signed N-bit range is enforced.	2026-06-24	7.8	CVE-2026-53036
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ocfs2: validate bg_bits during freefrag scan [BUG] A crafted filesystem can trigger an out-of-bounds bitmap walk when OCFS2_IOC_INFO is issued with OCFS2_INFO_FL_NON_COHERENT. BUG: KASAN: use-after-free in instrument_atomic_read include/linux/instrumented.h:68 [inline] BUG: KASAN: use-after-free in _test_bit include/asm-generic/bitops/instrumented-non-atomic.h:141 [inline] BUG: KASAN: use-after-free in test_bit_le include/asm-generic/bitops/le.h:21 [inline] BUG: KASAN: use-after-free in ocfs2_info_freefrag_scan_chain fs/ocfs2/ioctl.c:495 [inline] BUG: KASAN: use-after-free in ocfs2_info_freefrag_scan_bitmap fs/ocfs2/ioctl.c:588 [inline] BUG: KASAN: use-after-free in ocfs2_info_handle_freefrag fs/ocfs2/ioctl.c:662 [inline] BUG: KASAN: use-after-free in ocfs2_info_handle_request+0x1c66/0x3370 fs/ocfs2/ioctl.c:754 Read of size 8 at addr ffff888031bce000 by task syz.0.636/1435 Call Trace: __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0xbe/0x130 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xd1/0x650 mm/kasan/report.c:482 kasan_report+0xfb/0x140 mm/kasan/report.c:595 check_region_inline mm/kasan/generic.c:186 [inline] kasan_check_range+0x11c/0x200 mm/kasan/generic.c:200 __kasan_check_read+0x11/0x20 mm/kasan/shadow.c:31 instrument_atomic_read include/linux/instrumented.h:68 [inline] _test_bit include/asm-generic/bitops/instrumented-non-atomic.h:141 [inline] test_bit_le include/asm-generic/bitops/le.h:21 [inline] ocfs2_info_freefrag_scan_chain fs/ocfs2/ioctl.c:495 [inline] ocfs2_info_freefrag_scan_bitmap fs/ocfs2/ioctl.c:588 [inline] ocfs2_info_handle_freefrag fs/ocfs2/ioctl.c:662 [inline] ocfs2_info_handle_request+0x1c66/0x3370 fs/ocfs2/ioctl.c:754 ocfs2_info_handle+0x18d/0x2a0 fs/ocfs2/ioctl.c:828 ocfs2_ioctl+0x632/0x6e0 fs/ocfs2/ioctl.c:913 vfs_ioctl fs/ioctl.c:51 [inline] __do_sys_ioctl fs/ioctl.c:597 [inline] __se_sys_ioctl fs/ioctl.c:583 [inline] __x64_sys_ioctl+0x197/0x1e0 fs/ioctl.c:583 ... [CAUSE] ocfs2_info_freefrag_scan_chain() uses on-disk bg_bits directly as the bitmap scan limit. The coherent path reads group descriptors through ocfs2_read_group_descriptor(), which validates the descriptor before use. The non-coherent path uses ocfs2_read_blocks_sync() instead and skips that validation, so an impossible bg_bits value can drive the bitmap walk past the end of the block. [FIX] Compute the bitmap capacity from the filesystem format with ocfs2_group_bitmap_size(), report descriptors whose bg_bits exceeds that limit, and clamp the scan to the computed capacity. This keeps the freefrag report going while avoiding reads beyond the buffer.	2026-06-24	7.1	CVE-2026-53040

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix listxattr handling when the buffer is full [BUG] If an OCFS2 inode has both inline and block-based xattrs, listxattr() can return a size larger than the caller's buffer when the inline names consume that buffer exactly. kernel BUG at mm/usercopy.c:102! Oops: invalid opcode: 0000 [#1] SMP KASAN NOPTI RIP: 0010:usercopy_abort+0xb7/0xd0 mm/usercopy.c:102 Call Trace: __check_heap_object+0xe3/0x120 mm/slub.c:8243 check_heap_object mm/usercopy.c:196 [inline] __check_object_size mm/usercopy.c:250 [inline] __check_object_size+0x5c5/0x780 mm/usercopy.c:215 check_object_size include/linux/ucopysize.h:22 [inline] check_copy_size include/linux/ucopysize.h:59 [inline] copy_to_user include/linux/uaccess.h:219 [inline] listxattr+0xb0/0x170 fs/xattr.c:926 filename_listxattr fs/xattr.c:958 [inline] path_listxattr+0x137/0x320 fs/xattr.c:988 __do_sys_listxattr fs/xattr.c:1001 [inline] __se_sys_listxattr fs/xattr.c:998 [inline] __x64_sys_listxattr+0x7f/0xd0 fs/xattr.c:998 ... [CAUSE] Commit 936b8834366e ("ocfs2: Refactor xattr list and remove ocfs2_xattr_handler().") replaced the old per-handler list accounting with ocfs2_xattr_list_entry(), but it kept using size == 0 to detect probe mode. That assumption stops being true once ocfs2_listxattr() finishes the inline-xattr pass. If the inline names fill the caller buffer exactly, the block-xattr pass runs with a non-NULL buffer and a remaining size of zero. ocfs2_xattr_list_entry() then skips the bounds check, keeps counting block names, and returns a positive size larger than the supplied buffer. [FIX] Detect probe mode by testing whether the destination buffer pointer is NULL instead of whether the remaining size is zero. That restores the pre-refactor behavior and matches the OCFS2 getxattr helpers. Once the remaining buffer reaches zero while more names are left, the block-xattr pass now returns -ERANGE instead of reporting a size larger than the allocated list buffer.	2026-06-24	7.1	CVE-2026-53041
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: soc/tegra: cbb: Fix incorrect ARRAY_SIZE in fabric lookup tables Fix incorrect ARRAY_SIZE usage in fabric lookup tables which could cause out-of-bounds access during target timeout lookup.	2026-06-24	7.1	CVE-2026-53044
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: quota: Fix race of dquot_scan_active() with quota deactivation dquot_scan_active() can race with quota deactivation in quota_release_workfn() like: CPU0 (quota_release_workfn) CPU1 (dquot_scan_active) ===== ===== spin_lock(&dq_list_lock); list_replace_init(&releasing_dquots, &rls_head); /* dquot X on rls_head, dq_count == 0, DQ_ACTIVE_B still set */ spin_unlock(&dq_list_lock); synchronize_srcu(&dquot_srcu); spin_lock(&dq_list_lock); list_for_each_entry(dquot, &inuse_list, dq_inuse) { /* finds dquot X */ dquot_active(X) -> true atomic_inc(&X->dq_count); } spin_unlock(&dq_list_lock); spin_lock(&dq_list_lock); dquot = list_first_entry(&rls_head); WARN_ON_ONCE(atomic_read(&dquot->dq_count)); The problem is not only a cosmetic one as under memory pressure the caller of dquot_scan_active() can end up working on freed dquot. Fix the problem by making sure the dquot is removed from releasing list when we acquire a reference to it.	2026-06-24	7.8	CVE-2026-53050
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/msm: Fix VM_BIND UNMAP locking Wrong argument meant that the objs involved in UNMAP ops were not always getting locked. Since _NO_SHARE objs share a common resv with the VM (which is always locked) this would only show up with non-_NO_SHARE BOs. Patchwork: https://patchwork.freedesktop.org/patch/713898/	2026-06-24	7.8	CVE-2026-53054
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dm cache policy smq: fix missing locks in invalidating cache blocks In	2026-06-24	7.8	CVE-2026-53062

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	passthrough mode, the policy invalidate_mapping operation is called simultaneously from multiple workers, thus it should be protected by a lock. Otherwise, we might end up with data races on the allocated blocks counter, or even use-after-free issues with internal data structures when doing concurrent writes. Note that the existing FIXME in smq_invalidate_mapping() doesn't affect passthrough mode since migration tasks don't exist there, but would need attention if supporting fast device shrinking via suspend/resume without target reloading. Reproduce steps: 1. Create a cache device consisting of 1024 cache entries dmsetup create cmeta --table "0 8192 linear /dev/sdc 0" dmsetup create cdata --table "0 131072 linear /dev/sdc 8192" dmsetup create corig --table "0 262144 linear /dev/sdc 262144" dd if=/dev/zero of=/dev/mapper/cmeta bs=4k count=1 oflag=direct dmsetup create cache --table "0 262144 cache /dev/mapper/cmeta \ /dev/mapper/cdata /dev/mapper/corig 128 2 metadata2 writethrough smq 0" 2. Populate the cache, and record the number of cached blocks fio --name=populate --filename=/dev/mapper/cache --rw=randwrite --bs=4k \ --size=64m --direct=1 nr_cached=\$(dmsetup status cache awk '{split(\$7, a, "/"); print a[1]}') 3. Reload the cache into passthrough mode dmsetup suspend cache dmsetup reload cache --table "0 262144 cache /dev/mapper/cmeta \ /dev/mapper/cdata /dev/mapper/corig 128 2 metadata2 passthrough smq 0" dmsetup resume cache 4. Write to the passthrough cache. By setting multiple jobs with I/O size equal to the cache block size, cache blocks are invalidated concurrently from different workers. fio --filename=/dev/mapper/cache --name=test --rw=randwrite --bs=64k \ --direct=1 --numjobs=2 --randrepeat=0 --size=64m 5. Check if demoted matches cached block count. These numbers should match but may differ due to the data race. nr_demoted=\$(dmsetup status cache awk '{print \$12}') echo "\$nr_cached, \$nr_demoted"			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/komeda: fix integer overflow in AFBC framebuffer size check The AFBC framebuffer size validation calculates the minimum required buffer size by adding the AFBC payload size to the framebuffer offset. This addition is performed without checking for integer overflow. If the addition overflows, the size check may incorrectly succeed and allow userspace to provide an undersized drm_gem_object, potentially leading to out-of-bounds memory access. Add usage of check_add_overflow() to safely compute the minimum required size and reject the framebuffer if an overflow is detected. This makes the AFBC size validation more robust against malformed. Found by Linux Verification Center (linuxtesting.org) with SVACE.	2026-06-24	7.1	CVE-2026-53068
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net, bpf: fix null-ptr-deref in xdp_master_redirect() for down master syzkaller reported a kernel panic in bond_rr_gen_slave_id() reached via xdp_master_redirect(). Full decoded trace: https://syzkaller.appspot.com/bug?extid=80e046b8da2820b6ba73 bond_rr_gen_slave_id() dereferences bond->rr_tx_counter, a per-CPU counter that bonding only allocates in bond_open() when the mode is round-robin. If the bond device was never brought up, rr_tx_counter stays NULL. The XDP redirect path can still reach that code on a bond that was never opened: bpf_master_redirect_enabled_key is a global static key, so as soon as any bond device has native XDP attached, the XDP_TX -> xdp_master_redirect() interception is enabled for every slave system-wide. The path xdp_master_redirect() -> bond_xdp_get_xmit_slave() -> bond_xdp_xmit_roundrobin_slave_get() -> bond_rr_gen_slave_id() then runs against a bond that has no rr_tx_counter and crashes. Fix this in the generic xdp_master_redirect() by refusing to call into the master's ->ndo_xdp_get_xmit_slave() when the master device is not up. IFF_UP is only set after ->ndo_open() has successfully returned, so this reliably	2026-06-24	7.5	CVE-2026-53069

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	excludes masters whose XDP state has not been fully initialized. Drop the frame with XDP_ABORTED so the exception is visible via trace_xdp_exception() rather than silently falling through. This is not specific to bonding: any current or future master that defers XDP state allocation to ->ndo_open() is protected.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: sctp: disable BH before calling udp_tunnel_xmit_skb() udp_tunnel_xmit_skb() / udp_tunnel6_xmit_skb() are expected to run with BH disabled. After commit 6f1a9140ecda ("add xmit recursion limit to tunnel xmit functions"), on the path: udp(6)_tunnel_xmit_skb() -> ip(6)tunnel_xmit() dev_xmit_recursion_inc()/dec() must stay balanced on the same CPU. Without local_bh_disable(), the context may move between CPUs, which can break the inc/dec pairing. This may lead to incorrect recursion level detection and cause packets to be dropped in ip(6)_tunnel_xmit() or __dev_queue_xmit(). Fix it by disabling BH around both IPv4 and IPv6 SCTP UDP xmit paths. In my testing, after enabling the SCTP over UDP: # ip net exec ha sysctl -w net.sctp.udp_port=9899 # ip net exec ha sysctl -w net.sctp.encap_port=9899 # ip net exec hb sysctl -w net.sctp.udp_port=9899 # ip net exec hb sysctl -w net.sctp.encap_port=9899 # ip net exec ha iperf3 -s - without this patch: # ip net exec hb iperf3 -c 192.168.0.1 --sctp [5] 0.00-10.00 sec 37.2 MBytes 31.2 Mbits/sec sender [5] 0.00-10.00 sec 37.1 MBytes 31.1 Mbits/sec receiver - with this patch: # ip net exec hb iperf3 -c 192.168.0.1 --sctp [5] 0.00-10.00 sec 3.14 GBytes 2.69 Gbits/sec sender [5] 0.00-10.00 sec 3.14 GBytes 2.69 Gbits/sec receiver	2026-06-24	7.5	CVE-2026-53070
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix OOB in pcpu_init_value An out-of-bounds read occurs when copying element from a BPF_MAP_TYPE_CGROUP_STORAGE map to another pcpu map with the same value_size that is not rounded up to 8 bytes. The issue happens when: 1. A CGROUP_STORAGE map is created with value_size not aligned to 8 bytes (e.g., 4 bytes) 2. A pcpu map is created with the same value_size (e.g., 4 bytes) 3. Update element in 2 with data in 1 pcpu_init_value assumes that all sources are rounded up to 8 bytes, and invokes copy_map_value_long to make a data copy, However, the assumption doesn't stand since there are some cases where the source may not be rounded up to 8 bytes, e.g., CGROUP_STORAGE, skb->data. the verifier verifies exactly the size that the source claims, not the size rounded up to 8 bytes by kernel, an OOB happens when the source has only 4 bytes while the copy size(4) is rounded up to 8.	2026-06-24	7.1	CVE-2026-53076
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/rds: Restrict use of RDS/IB to the initial network namespace Prevent using RDS/IB in network namespaces other than the initial one. The existing RDS/IB code will not work properly in non-initial network namespaces.	2026-06-24	7.8	CVE-2026-53077
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix same-register dst/src OOB read and pointer leak in sock_ops When a BPF sock_ops program accesses ctx fields with dst_reg == src_reg, the SOCK_OPS_GET_SK() and SOCK_OPS_GET_FIELD() macros fail to zero the destination register in the !fullsock / !locked_tcp_sock path. Both macros borrow a temporary register to check is_fullsock / is_locked_tcp_sock when dst_reg == src_reg, because dst_reg holds the ctx pointer. When the check is false (e.g., TCP_NEW_SYN_RECV state with a request_sock), dst_reg should be zeroed but is not, leaving the stale ctx pointer: - SOCK_OPS_GET_SK: dst_reg retains the ctx pointer, passes NULL checks as PTR_TO_SOCKET_OR_NULL, and can be used as a bogus socket pointer, leading to stack-out-of-bounds access in helpers like bpf_skc_to_tcp6_sock(). - SOCK_OPS_GET_FIELD: dst_reg retains the ctx pointer which the verifier believes is a SCALAR_VALUE, leaking a kernel pointer. Fix both macros by: - Changing JMP_A(1) to JMP_A(2) in the fullsock path to skip the added instruction. - Adding BPF_MOV64_IMM(si-	2026-06-24	7.8	CVE-2026-53078

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	>dst_reg, 0) after the temp register restore in the !fullsock path, placed after the restore because dst_reg == src_reg means we need src_reg intact to read ctx->temp.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Enforce regsafe base id consistency for BPF_ADD_CONST scalars When regsafe() compares two scalar registers that both carry BPF_ADD_CONST, check_scalar_ids() maps their full compound id (aka base BPF_ADD_CONST flag) as one idmap entry. However, it never verifies that the underlying base ids, that is, with the flag stripped are consistent with existing idmap mappings. This allows construction of two verifier states where the old state has R3 = R2 + 10 (both sharing base id A) while the current state has R3 = R4 + 10 (base id C, unrelated to R2). The idmap creates two independent entries: A->B (for R2) and A flag->C flag (for R3), without catching that A->C conflicts with A->B. State pruning then incorrectly succeeds. Fix this by additionally verifying base ID mapping consistency whenever BPF_ADD_CONST is set: after mapping the compound ids, also invoke check_ids() on the base IDs (flag bits stripped). This ensures that if A was already mapped to B from comparing the source register, any ADD_CONST derivative must also derive from B, not an unrelated C.	2026-06-24	7.8	CVE-2026-53081
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: fix mm lifecycle in open-coded task_vma iterator The open-coded task_vma iterator reads task->mm locklessly and acquires mmap_read_trylock() but never calls mmget(). If the task exits concurrently, the mm_struct can be freed as it is not SLAB_TYPESAFE_BY_RCU, resulting in a use-after-free. Safely read task->mm with a trylock on alloc_lock and acquire an mm reference. Drop the reference via bpf_iter_mmpout_async() in _destroy() and error paths. bpf_iter_mmpout_async() is a local wrapper around mmpout_async() with a fallback to mmpout() on !CONFIG_MMU. Reject irq-disabled contexts (including NMI) up front. Operations used by _next() and _destroy() (mmap_read_unlock, bpf_iter_mmpout_async) take spinlocks with IRQs disabled (pool->lock, pi_lock). Running from NMI or from a tracepoint that fires with those locks held could deadlock. A trylock on alloc_lock is used instead of the blocking task_lock() (get_task_mm) to avoid a deadlock when a softirq BPF program iterates a task that already holds its alloc_lock on the same CPU.	2026-06-24	7.8	CVE-2026-53085
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: bcmgenet: fix leaking free_bds While reclaiming the tx queue we fast forward the write pointer to drop any data in flight. These dropped frames are not added back to the pool of free bds. We also need to tell the netdev that we are dropping said data.	2026-06-24	7.5	CVE-2026-53087
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix ld_{abs,ind} failure path analysis in subprogs Usage of ld_{abs,ind} instructions got extended into subprogs some time ago via commit 09b28d76eac4 ("bpf: Add abnormal return checks."). These are only allowed in subprograms when the latter are BTF annotated and have scalar return types. The code generator in bpf_gen_ld_abs() has an abnormal exit path (r0=0 + exit) from legacy cBPF times. While the enforcement is on scalar return types, the verifier must also simulate the path of abnormal exit if the packet data load via ld_{abs,ind} failed. This is currently not the case. Fix it by having the verifier simulate both success and failure paths, and extend it in similar ways as we do for tail calls. The success path (r0=unknown, continue to next insn) is pushed onto stack for later validation and the r0=0 and return to the caller is done on the fall-through side.	2026-06-24	7.8	CVE-2026-53090
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix linked reg delta tracking when src_reg == dst_reg Consider the case of rX += rX where src_reg and dst_reg are pointers to the same bpf_reg_state in adjust_reg_min_max_vals(). The latter first modifies the dst_reg in-place,	2026-06-24	7.8	CVE-2026-53092

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and later in the delta tracking, the subsequent <code>is_reg_const(src_reg)/reg_const_value(src_reg)</code> reads the post-{add,sub} value instead of the original source. This is problematic since it sets an incorrect delta, which <code>sync_linked_regs()</code> then propagates to linked registers, thus creating a verifier-vs-runtime mismatch. Fix it by just skipping this corner case.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix stale offload->prog pointer after constant blinding When a dev-bound-only BPF program (BPF_F_XDP_DEV_BOUND_ONLY) undergoes JIT compilation with constant blinding enabled (<code>bpf_jit_harden >= 2</code>), <code>bpf_jit_blind_constants()</code> clones the program. The original prog is then freed in <code>bpf_jit_prog_release_other()</code> , which updates <code>aux->prog</code> to point to the surviving clone, but fails to update <code>offload->prog</code> . This leaves <code>offload->prog</code> pointing to the freed original program. When the network namespace is subsequently destroyed, <code>cleanup_net()</code> triggers <code>bpf_dev_bound_netdev_unregister()</code> , which iterates <code>ondev->progs</code> and calls <code>__bpf_prog_offload_destroy(offload->prog)</code> . Accessing the freed prog causes a page fault: BUG: unable to handle page fault for address: ffffc900085f1038 Workqueue: netns cleanup_net RIP: 0010: __bpf_prog_offload_destroy+0xc/0x80 Call Trace: __bpf_offload_dev_netdev_unregister+0x257/0x350 bpf_dev_bound_netdev_unregister+0x4a/0x90 unregister_netdevice_many_notify+0x2a2/0x660 ... cleanup_net+0x21a/0x320 The test sequence that triggers this reliably is: 1. Set <code>net.core.bpf_jit_harden=2</code> (<code>echo 2 > /proc/sys/net/core/bpf_jit_harden</code>) 2. Run <code>xdp_metadata selftest</code> , which creates a dev-bound-only XDP program on a veth inside a netns (<code>./test_progs -t xdp_metadata</code>) 3. <code>cleanup_net -></code> page fault in <code>__bpf_prog_offload_destroy</code> Dev-bound-only programs are unique in that they have an offload structure but go through the normal JIT path instead of <code>bpf_prog_offload_compile()</code> . This means they are subject to constant blinding's prog clone-and-replace, while also having <code>offload->prog</code> that must stay in sync. Fix this by updating <code>offload->prog</code> in <code>bpf_jit_prog_release_other()</code> , alongside the existing <code>aux->prog</code> update. Both are back-pointers to the prog that must be kept in sync when the prog is replaced.	2026-06-24	7.8	CVE-2026-53094
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Use RCU-safe iteration in <code>dev_map_redirect_multi()</code> SKB path The <code>DEVMAP_HASH</code> branch in <code>dev_map_redirect_multi()</code> uses <code>hlist_for_each_entry_safe()</code> to iterate hash buckets, but this function runs under RCU protection (called from <code>xdp_do_generic_redirect_map()</code> in softirq context). Concurrent writers (<code>__dev_map_hash_update_elem</code> , <code>dev_map_hash_delete_elem</code>) modify the list using RCU primitives (<code>hlist_add_head_rcu</code> , <code>hlist_del_rcu</code>). <code>hlist_for_each_entry_safe()</code> performs plain pointer dereferences without <code>rcu_dereference()</code> , missing the acquire barrier needed to pair with writers' <code>rcu_assign_pointer()</code> . On weakly-ordered architectures (ARM64, POWER), a reader can observe a partially-constructed node. It also defeats <code>CONFIG_PROVE_RCU</code> lockdep validation and KCSAN data-race detection. Replace with <code>hlist_for_each_entry_rcu()</code> using <code>rcu_read_lock_bh_held()</code> as the lockdep condition, consistent with the <code>rcu_dereference_check()</code> used in the <code>DEVMAP</code> (non-hash) branch of the same functions. Also fix the same incorrect lockdep_is_held(&dtab->index_lock) condition in <code>dev_map_enqueue_multi()</code> , where the lock is not held either.	2026-06-24	7.8	CVE-2026-53096
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: s390/bpf: Zero-extend bpf prog return values and kfunc arguments s390x ABI requires callers to zero-extend unsigned arguments and sign-extend signed arguments, and callees to zero-extend unsigned return values and	2026-06-24	7.8	CVE-2026-53110

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sign-extend signed return values. s390 BPF JIT currently implements only sign extension. Fix this omission and implement zero extension too.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: fs/omfs: reject s_sys_blocksize smaller than OMFS_DIR_START omfs_fill_super() rejects oversized s_sys_blocksize values (> PAGE_SIZE), but it does not reject values smaller than OMFS_DIR_START (0x1b8 = 440). Later, omfs_make_empty() uses sbi->s_sys_blocksize - OMFS_DIR_START as the length argument to memset(). Since s_sys_blocksize is u32, a crafted filesystem image with s_sys_blocksize < OMFS_DIR_START causes an unsigned underflow there, wrapping to a value near 2^32. That drives a ~4 GiB memset() from bh->b_data + OMFS_DIR_START and overwrites kernel memory far beyond the backing block buffer. Add the corresponding lower-bound check alongside the existing upper-bound check in omfs_fill_super(), so that malformed images are rejected during superblock validation before any filesystem data is processed.	2026-06-24	7.8	CVE-2026-53130
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: vsock/virtio: fix potential unbounded skb queue virtio_transport_inc_rx_pkt() checks vvs->rx_bytes + len > vvs->buf_alloc. virtio_transport_recv_enqueue() skips coalescing for packets with VIRTIO_VSOCK_SEQ_EOM. If fed with packets with len == 0 and VIRTIO_VSOCK_SEQ_EOM, a very large number of packets can be queued because vvs->rx_bytes stays at 0. Fix this by estimating the skb metadata size: (Number of skbs in the queue) * SKB_TRUESIZE(0)	2026-06-25	7.1	CVE-2026-53132
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/umem: Fix truncation for block sizes >= 4G When the iommu is used the linearization of the mapping can give a single block that is very large split across multiple SG entries. When __rdma_block_iter_next() reassembles the split SG entries it is overflowing the 32 bit stack values and computed the wrong DMA addresses for blocks after the truncation. Use the right types to hold DMA addresses.	2026-06-25	7.8	CVE-2026-53133
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/gem: Try to fix change_handle ioctl, attempt 4 [airlied: just added some comments on how to reenale] On-list because the cat is out of the bag and we're clearly not good enough to figure this out in private. The story thus far: 5e28b7b94408 ("drm: Set old handle to NULL before prime swap in change_handle") tried to fix a race condition between the gem_close and gem_change_handle ioctls, but got a few things wrong: - There's a confusion with the local variable handle, which is actually the new handle, and so the two-stage trick was actually applied to the wrong idr slot. 7164d78559b0 ("drm/gem: fix race between change_handle and handle_delete") tried to fix that by adding yet another code block, but forgot to add the error handling. Which meant we now have two paths, both kinda wrong. - dc366607c41c ("drm: Replace old pointer to new idr") tried to apply another fix, but inconsistently, again because of the handle confusion - this would be the right fix (kinda, somewhat, it's a mess) if we'd do the two-stage approach for the new handle. Except that wasn't the intent of the original fix. We also didn't have an igt merged for the original ioctl, which is a big no-go. This was attempted to address off-list in the original bugfix, and amd QA people claimed the bug was fixed now. Very clearly that's not the case. Here's my attempt to sort this out: - Rename the local variable to new_handle, the old aliasing with args->handle is just too dangerously confusing. - Merge the gem obj lookup with the two-stage idr_replace so that we avoid getting ourselves confused there. - This means we don't have a surplus temporary reference anymore, only an inherited from the idr. A concurrent gem_close on the new_handle could steal that. Fix that with the same two-stage approach create_tail uses. This is a bit overkill as documented in the comment, but I also don't trust my ability to understand this all correctly, so go with the established pattern we have from other ioctls instead for maximum	2026-06-25	7.8	CVE-2026-53145

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	paranoia. - Adjust error paths. I've tried to make the error and success paths common, because they are identical except for which handle is removed and on which we call idr_replace to (re)install the object again. But that made things messier to read, so I've left it at the more verbose version, which unfortunately hides the symmetry in the entire code flow a bit. - While at it, also replace the 7 space indent with 1 tab. And finally, because I flat out don't trust my abilities here at all anymore: - Disable the ioctl until we have the igt situation and everything else sorted out on-list and with full consensus. v2: Sashiko noticed that I didn't handle the error path for idr_replace correctly, it must be checked with IS_ERR_OR_NULL like in gem_handle_delete. So yeah, definitely should just the existing paths 1:1 because this is endless amounts of tricky. Also add the Fixes: line for the original ioctl, I forgot that too.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Limit XDomain response copy to actual frame size tb_xdomain_copy() copies req->response_size bytes from the received packet buffer regardless of the actual frame size. When a short response arrives, this reads past the valid frame data in the DMA pool buffer into stale contents from previous transactions. Use the minimum of frame size and expected response size for the copy length.	2026-06-25	7.1	CVE-2026-53146
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mm/list_lru: drain before clearing xarray entry on reparent memcg_reparent_list_lrus() clears the dying memcg's xarray entry with xas_store(&xas, NULL) before reparenting its per-node lists into the parent. This opens a window where a concurrent list_lru_del() arriving for the dying memcg sees xa_load() == NULL, walks to the parent in lock_list_lru_of_memcg(), takes the parent's per-node lock, and calls list_del_init() on an item still physically linked on the dying memcg's list. If another in-flight thread holds the dying memcg's per-node lock at the same moment (another list_lru_del, or a list_lru_walk_one running an isolate callback), both threads modify ->next/->prev pointers on the same physical list under different locks. Adjacent items can corrupt each other's links. Fix it by reversing the order: reparent each per-node list and mark the child's list lru dead and then clear the xarray entry. Any concurrent list_lru op that finds the still-set xarray entry either takes the dying memcg's per-node lock (synchronizing with the drain) or sees LONG_MIN and walks to the parent, where the items now live.	2026-06-25	7.8	CVE-2026-53153
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: misc: fastrpc: fix use-after-free race in fastrpc_map_create fastrpc_map_lookup returns a raw pointer after releasing fl->lock. The caller fastrpc_map_create then calls fastrpc_map_get (kref_get_unless_zero) on this unprotected pointer. A concurrent MEM_UNMAP can free the map between the lock release and the kref operation, resulting in a use-after-free on the freed slab object. Restore the take_ref parameter to fastrpc_map_lookup so the reference is acquired atomically under fl->lock before the pointer is exposed to the caller.	2026-06-25	7.8	CVE-2026-53160
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: misc: fastrpc: fix use-after-free of fastrpc_user in workqueue context There is a race between fastrpc_device_release() and the workqueue that processes DSP responses. When the user closes the file descriptor, fastrpc_device_release() frees the fastrpc_user structure. Concurrently, an in-flight DSP invocation can complete and fastrpc_rpmsg_callback() schedules context cleanup via schedule_work(&ctx->put_work). If the workqueue runs fastrpc_context_free() in parallel with or after fastrpc_device_release() has freed the user structure, it dereferences the freed fastrpc_user. Depending on the state of the context at the time of the race, any one of the following accesses can be hit: 1. fastrpc_buf_free() calls fastrpc_ipa_to_dma_addr(buf->fl->cctx, ...) to strip the SID bits from the stored IOVA before passing the physical address to	2026-06-25	7.8	CVE-2026-53161

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	dma_free_coherent(). 2. fastrpc_free_map() reads map->fl->cctx->vmperms[0].vmid to reconstruct the source permission bitmask needed for the qcom_scm_assign_mem() call that returns memory from the DSP VM back to HLOS. 3. fastrpc_free_map() acquires map->fl->lock to safely remove the map node from the fl->maps list. The resulting use-after-free manifests as: pc : fastrpc_buf_free+0x38/0x80 [fastrpc] lr : fastrpc_context_free+0xa8/0x1b0 [fastrpc] fastrpc_context_free+0xa8/0x1b0 [fastrpc] fastrpc_context_put_wq+0x78/0xa0 [fastrpc] process_one_work+0x180/0x450 worker_thread+0x26c/0x388 Add kref-based reference counting to fastrpc_user. Have each invoke context take a reference on the user at allocation time and release it when the context is freed. Release the initial reference in fastrpc_device_release() at file close. Move the teardown of the user structure - freeing pending contexts, maps, mmmaps, and the channel context reference - into the kref release callback fastrpc_user_free(), so that it runs only when the last reference is dropped, regardless of whether that happens at device close or after the final in-flight context completes.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: memcg: use round-robin victim selection in refill_stock Harry Yoo reported that get_random_u32_below() is not safe to call in the nmi context and memcg charge draining can happen in nmi context. More specifically get_random_u32_below() is neither reentrant- nor NMI-safe: it acquires a per-cpu local_lock via local_lock_irqsave() on the batched_entropy_u32 state. An NMI that lands on a CPU mid-update of the ChaCha batch state and recurses into the random subsystem would corrupt that state. The memcg_stock local_trylock prevents re-entry on the percpu stock itself, but cannot protect an unrelated subsystem's per-cpu lock. Replace the random pick with a per-cpu round-robin counter stored in memcg_stock_pcp and serialized by the same local_trylock that already guards cached[] and nr_pages[]. No atomics, no random calls, no extra locks needed.	2026-06-25	7.8	CVE-2026-53162
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: iomap: avoid potential null folio->mapping deref during error reporting When a buffered read fails, iomap_finish_folio_read() reports the error with fserror_report_io(folio->mapping->host, ...). This is called after ifs->read_bytes_pending has been decremented by the bytes attempted to be read. For a folio split across multiple read completions, the folio is only guaranteed to stay locked while read_bytes_pending > 0. Once iomap_finish_folio_read() decrements read_bytes_pending, another in-flight read can complete and end the read on the folio, which unlocks it. This allows truncate logic to run and detach the folio (set folio->mapping to NULL). The error reporting path then can dereference a NULL folio->mapping. As reported by Sam Sun, this is the race that can occur: CPU0: failed completion CPU1: final completion CPU2: truncate ----- read_bytes_pending -= len finished = false /* preempted before fserror_report_io() */ read_bytes_pending -= len finished = true folio_end_read() truncate clears folio->mapping fserror_report_io(folio->mapping->host, ...) ^ NULL deref Fix this by reporting the error first before decrementing ifs->read_bytes_pending.	2026-06-25	7.5	CVE-2026-53165
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/ethosu: fix IFM region index out-of-bounds in command stream parser NPU_SET_IFM_REGION extracts the region index with param & 0x7f, giving a maximum value of 127. However region_size[] and output_region[] in struct ethosu_validated_cmdstream_info are both sized to NPU_BASEP_REGION_MAX (8), giving valid indices [0..7]. Every other region assignment in the same switch uses param & 0x7: NPU_SET_OFM_REGION: st.ofm.region = param & 0x7; NPU_SET_IFM2_REGION: st.ifm2.region = param & 0x7;	2026-06-25	7.8	CVE-2026-53172

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	NPU_SET_WEIGHT_REGION: st.weight[0].region = param & 0x7; NPU_SET_SCALE_REGION: st.scale[0].region = param & 0x7; The 0x7f mask on IFM is inconsistent and appears to be a typo. feat_matrix_length() and calc_sizes() use the region index directly as an array subscript into the kzalloc'd info struct: info->region_size[fm->region] = max(...); A userspace caller supplying NPU_SET_IFM_REGION with param > 7 causes a write up to 127*8 = 1016 bytes past the start of region_size[], corrupting adjacent kernel heap data. Fix by applying the same & 0x7 mask used by all other region assignments.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/ethosu: fix OOB write in ethosu_gem_cmdstream_copy_and_validate() The command stream parsing loop increments the index variable a second time when a 64-bit command word is encountered (bit 14 set), but does not re-check the loop bound before writing the second word: for (i = 0; i < size / 4; i++) { bocmds[i] = cmds[0]; if (cmd & 0x4000) { i++; bocmds[i] = cmds[1]; /* unchecked */ } } The buffer bocmds is backed by a DMA allocation of exactly size bytes from drm_gem_dma_create(ddev, size), giving valid indices [0, size/4-1]. When i == size/4 - 1 on entry to an iteration and bit 14 of cmds[0] is set, bocmds[size/4-1] is written in bounds, i is then incremented to size/4, and bocmds[size/4] writes four bytes past the end of the allocation. Userspace controls both the buffer contents and the size argument via the ioctl, making this a userspace-triggerable heap out-of-bounds write. Fix by checking the incremented index against the buffer bound before the second write and returning -EINVAL if the buffer is too small to contain the extended command.	2026-06-25	7.8	CVE-2026-53173
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ovl: keep err zero after successful ovl_cache_get() ovl_iterate_merged() stores PTR_ERR(cache) in err before checking IS_ERR(cache). On success err holds the truncated cache pointer and can be returned as a bogus non-zero error. The syzbot reproducer reaches this through overlay-on-overlay readdir: getdents64 iterate_dir(outer overlay file) ovl_iterate_merged() ovl_cache_get() ovl_dir_read_merged() ovl_dir_read() iterate_dir(inner overlay file) ovl_iterate_merged() Only compute PTR_ERR(cache) on the error path.	2026-06-25	7.8	CVE-2026-53174
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: timers/migration: Fix livelock in tmigr_handle_remote_up() tmigr_handle_remote_cpu() skips timer_expire_remote() when cpu == smp_processor_id(), assuming the local softirq path already handled this CPU's timers. This assumption is wrong because jiffies can advance after the handling of the CPU's global timers in run_timer_base(BASE_GLOBAL) and before tmigr_handle_remote() evaluates the expiry times. As a consequence a timer which expires after the CPU local timer wheel advanced and becomes expired in the remote handling is ignored and the callback is never invoked and removed from the timer wheel. What's worse is that fetch_next_timer_interrupt_remote() keeps reporting it as expired, and the event is re-queued with expires == now on each iteration. The goto-again loop spins indefinitely. Fix this by calling timer_expire_remote() unconditionally. That's minimal overhead for the common case as __run_timer_base() returns immediately if there is nothing to expire in the local wheel. [tgix: Amend change log and add a comment]	2026-06-25	7.5	CVE-2026-53180
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: nl80211: reject oversized EMA RNR lists nl80211_parse_rnr_elems() stores the parsed element count in a u8-backed cfg80211_rnr_elems::cnt field and uses that count to size the flexible array allocation. Reject nested NL80211_ATTR_EMA_RNR_ELEMS input once the count reaches 255, before incrementing it again. This keeps the parser aligned with the data	2026-06-25	7.8	CVE-2026-53182

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	structure it fills and matches the existing bound check used by nl80211_parse_mbssid_elems().			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mptcp: allow subflow rcv wnd to shrink In MPTCP connection, the `window` field in the TCP header refers to the MPTCP-level rcv_nxt and it's right edge should not move backward. Such constraint is enforced at DSS option generation time. At the same time, the TCP stack ensures independently that the TCP-level rcv wnd right's edge does not move backward. That in turn causes artificial inflating of the MPTCP rcv window when the incoming data is acked at the TCP level and is OoO in the MPTCP sequence space (or lands in the backlog). As a consequence, the incoming traffic can exceed the receiver rcvbuf size even when the sender is not misbehaving. Prevent such scenario forcibly allowing the TCP subflow to shrink the TCP-level rcv wnd regardless of the current netns setting.	2026-06-25	7.5	CVE-2026-53183
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: udp: clear skb->dev before running a sockmap verdict On the UDP receive path skb->dev is repurposed as dev_scratch (the truesize/state cache set by udp_set_dev_scratch()), through the union { struct net_device *dev; unsigned long dev_scratch; } in sk_buff. When a UDP socket is in a sockmap, sk_data_ready is sk_psock_verdict_data_ready(), which calls udp_read_skb() -> recv_actor() (sk_psock_verdict_rcv) to run the attached SK_SKB verdict program in softirq. If that program calls a socket-lookup helper (bpf_sk_lookup_tcp/udp, bpf_skc_lookup_tcp), bpf_skc_lookup() does: if (skb->dev) caller_net = dev_net(skb->dev); skb->dev still holds the dev_scratch value (a non-NULL integer), so dev_net() dereferences it as a struct net_device * and the kernel takes a general protection fault on a non-canonical address in softirq: Oops: general protection fault, probably for non-canonical address 0x1010000800004a0 CPU: 1 UID: 0 PID: 1406 Comm: syz.2.19 Not tainted 7.1.0-rc6 #1 PREEMPT(full) RIP: 0010:bpf_skc_lookup net/core/filter.c:7033 [inline] RIP: 0010:bpf_sk_lookup+0x45/0x160 net/core/filter.c:7047 Call Trace: <IRQ> bpf_prog_4675cb904b7071f8+0x12e/0x14e bpf_prog_run_pin_on_cpu+0xc6/0x1f0 sk_psock_verdict_rcv+0x1ba/0x350 udp_read_skb+0x31a/0x370 sk_psock_verdict_data_ready+0x2e3/0x600 __udp_enqueue_schedule_skb+0x4c8/0x650 udpv6_queue_rcv_one_skb+0x3ec/0x740 udp6_unicast_rcv_skb+0x11d/0x140 ip6_protocol_deliver_rcu+0x61e/0x950 ip6_input_finish+0xa9/0x150 NF_HOOK+0x286/0x2f0 ip6_input+0x117/0x220 NF_HOOK+0x286/0x2f0 __netif_receive_skb+0x85/0x200 process_backlog+0x374/0x9a0 __napi_poll+0x4f/0x1c0 net_rx_action+0x3b0/0x770 handle_softirqs+0x15a/0x460 do_softirq+0x57/0x80 </IRQ> The rmem charge that dev_scratch accounted for is released by skb_rcv_udp() on dequeue, just above, so the scratch is dead by the time recv_actor() runs. Clear skb->dev so bpf_skc_lookup() falls back to sock_net(skb->sk), which skb_set_owner_sk_safe() set just above.	2026-06-25	7.5	CVE-2026-53184
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: zram: fix use-after-free in zram_bvec_write_partial() zram_read_page() picks the sync or async backing device read path based on whether the parent bio is NULL. zram_bvec_write_partial() passes its parent bio down, so for ZRAM_WB slots the read is dispatched asynchronously and zram_read_page() returns 0 while the bio is still in flight. The caller then runs memcpy_from_bvec(), zram_write_page() and __free_page() on the buffer, leaving the async read to write into a freed page. zram_bvec_read_partial() was switched to NULL in commit 4e3c87b9421d ("zram: fix synchronous reads") for the same reason; the write_partial counterpart was missed.	2026-06-25	7.8	CVE-2026-53185

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/core: Validate cpu_id against nr_cpu_ids in DMAH alloc The cpu_id attribute supplied by user space through UVERBS_ATTR_ALLOC_DMAH_CPU_ID is passed directly to cpumask_test_cpu() without first verifying that the value is within the valid CPU range. Passing such untrusted data to cpumask_test_cpu() may lead to an out-of-bounds read of the underlying cpumask bitmap: the helper expands to a test_bit() that indexes the bitmap by cpu_id / BITS_PER_LONG with no bound check. In addition, on kernels built with CONFIG_DEBUG_PER_CPU_MAPS it trips the WARN_ON_ONCE() in cpumask_check(); combined with panic_on_warn this turns a bad user input into a machine reboot. Reject any cpu_id that is not smaller than nr_cpu_ids with -EINVAL before it is used. Reported by Smatch.	2026-06-25	7.1	CVE-2026-53187
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: mm/huge_memory: update file PMD counter before folio_put() __split_huge_pmd_locked() updates the file/shmem RSS counter after dropping the PMD mapping's folio reference. If folio_put() drops the last reference, mm_counter_file() can later read freed folio state via folio_test_swapbacked(). Move the counter update before folio_put().	2026-06-25	7.8	CVE-2026-53189
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: io_uring/net: inherit IORING_CQE_F_BUF_MORE across bundle recv retries When a bundle recv retries inside io_recv_finish(), the merge logic OR the saved cflags from the previous iteration with the cflags returned by the new iteration: cflags = req->cqe.flags (cflags & CQE_F_MASK); Bits listed in CQE_F_MASK are inherited from the new iteration, and all other bits (notably IORING_CQE_F_BUFFER and the buffer ID) come from the saved cflags. Before this change CQE_F_MASK covered only IORING_CQE_F_SOCKET_NONEMPTY and IORING_CQE_F_MORE. When using provided buffer rings (IOU_PBUF_RING_INC) with incremental mode, and bundle recv, io_kbuf_inc_commit() can leave the head ring entry partially consumed, __io_put_kbufs() then sets IORING_CQE_F_BUF_MORE on the returned cflags so userspace knows the buffer ID will be reused for subsequent completions. Because IORING_CQE_F_BUF_MORE was not in CQE_F_MASK, the merge above silently dropped it whenever the final retry iteration partially consumed the buffer, and the subsequent req->cqe.flags = cflags & ~CQE_F_MASK save would have left a stale IORING_CQE_F_BUF_MORE in the carried-over cflags had one been present. Userspace would then wrongfully advance it ring head past an entry the kernel still uses. Add IORING_CQE_F_BUF_MORE to CQE_F_MASK so it is both inherited from the new iteration into the user-visible CQE and stripped from the saved cflags between iterations.	2026-06-25	7.8	CVE-2026-53191
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: timer: Fix UAF at snd_timer_user_params() At releasing a timer object, e.g. when a userspace timer (CONFIG_SND_UTIMER) gets closed and snd_timer_free() is called, it tries to detach the timer instances and release the resources. However, it's still possible that other in-flight tasks are holding the timer instance where the to-be-deleted timer object is associated, and this may lead to racy accesses. Fortunately, most of ioctls dealing with the timer instance list already have the protection with register_mutex, and this also avoids such races. But, SNDRV_TIMER_IOCTL_PARAMS isn't protected, hence the concurrent ioctl may lead to use-after-free. This patch just adds the guard with register_mutex to protect snd_timer_user_params() for covering the code path as a quick workaround. It's no hot-path but rather a rarely issued ioctl, so the performance penalty doesn't matter.	2026-06-25	7.8	CVE-2026-53192
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: timer: Forcibly close timer instances at closing When snd_timer object is freed via snd_timer_free() and still pending snd_timer_instance objects	2026-06-25	7.8	CVE-2026-53193

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	are assigned to the timer object, it tries to unlink all instances and just set NULL to each ti->timer, then releases the resources immediately. The problem is, however, when there are slave timer instances that are associated with a master instance linked to this timer: namely, those slave instances still point to the freed timer object although the master instance is unlinked, which may lead to user-after-free. The bug can be easily triggered particularly when a new userspace-driven timers (CONFIG_SND_UTIMER) is involved, since it can create and delete the timer object via a simple file open/close, while the other applications may keep accessing to that timer. This patch is an attempt to paper over the problem above: now instead of just unlinking, call snd_timer_close[_locked]() forcibly for each pending timer instance, so that all assigned slave timer instances are properly detached, too. Since snd_timer_close() might be called later by the driver that created that instance, the check of SNDRV_TIMER_IFLG_DEAD is added at the beginning, too.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: USB: serial: k15kusb105: fix bulk-out buffer overflow klsi_105_prepare_write_buffer() is called by the generic write path with the bulk-out buffer and its size (bulk_out_size, 64 bytes). It stores a two-byte length header at the start of the buffer and copies the payload from the write fifo starting at buf + KLSI_HDR_LEN, but passes the full buffer size as the number of bytes to copy: count = kfifo_out_locked(&port->write_fifo, buf + KLSI_HDR_LEN, size, &port->lock); When the fifo holds at least size bytes, size bytes are copied starting two bytes into the size-byte buffer, writing KLSI_HDR_LEN bytes past its end. Copy at most size - KLSI_HDR_LEN bytes instead, leaving room for the header as safe_serial already does. Writing bulk_out_size or more bytes to the tty triggers a slab out-of-bounds write, observed with KASAN by emulating the device with dummy_hcd and raw-gadget: BUG: KASAN: slab-out-of-bounds in kfifo_copy_out+0x83/0xc0 Write of size 64 at addr ffff888112c62202 by task python3 kfifo_copy_out klsi_105_prepare_write_buffer [k15kusb105] usb_serial_generic_write_start [usbserial] Allocated by task 139: usb_serial_probe [usbserial] The buggy address is located 2 bytes inside of allocated 64-byte region The out-of-bounds write no longer occurs with this change applied.	2026-06-25	7.8	CVE-2026-53194
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: hv_netvsc: use kmap_local_page in netvsc_copy_to_send_buf netvsc_copy_to_send_buf() copies page buffer entries into the VMBus send buffer using phys_to_virt() on the entry PFN. Entries for the RNDIS header and the skb linear data come from kmalloc'd memory and are always in the kernel direct map, but entries for skb fragments reference page cache or user pages, which on 32-bit x86 with CONFIG_HIGHMEM=y can live above the LOWMEM boundary. For such a page phys_to_virt() returns an address outside the direct map and the subsequent memcpy() faults on the transmit softirq path, which is fatal. Map the pages with kmap_local_page() instead, handling two properties of the page buffer entries: - pb[i].pfn is a Hyper-V PFN at HV_HYP_PAGE_SIZE (4K) granularity, not a native PFN. Reconstruct the physical address first and derive the native page from it, so the mapping stays correct where PAGE_SIZE > HV_HYP_PAGE_SIZE (e.g. arm64 with 64K pages). - Since commit 41a6328b2c55 ("hv_netvsc: Preserve contiguous PFN grouping in the page buffer array"), an entry describes a full physically contiguous fragment and pb[i].len can exceed PAGE_SIZE, while kmap_local_page() maps a single page. Copy page by page, splitting at native page boundaries. The copy path only handles packets smaller than the send section size (6144 bytes by default); larger packets take the cp_partial path where only the RNDIS header is copied. So entries here are bounded by the section size and a copy is split at most once on 4K-page systems. On !CONFIG_HIGHMEM	2026-06-25	7.5	CVE-2026-53199

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	configs kmap_local_page() folds to page_address() and no mapping work is added.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Revert "drm/xe: Skip exec queue schedule toggle if queue is idle during suspend" This reverts commit 8533051ce92015e9cc6f75e0d52119b9d91610b6. The idle-skip optimization bypasses GuC suspend, so the GPU may not perform the context switch that flushes TLB entries for invalidated userptr VMAs. In LR/preempt-fence VM mode, this can lead to missed TLB invalidation and page faults during userptr invalidation tests. Restore unconditional schedule toggling on suspend so the context-switch TLB flush is always performed. This optimization will be reintroduced with a fix that does not skip suspend in LR/preempt-fence VM mode. (cherry picked from commit 6a1e7934d9a6cf46aeca00a99c2603d1295e170)	2026-06-25	7.8	CVE-2026-53201
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/ivpu: Fix signed integer truncation in IPC receive Fix potential buffer overflow where firmware-supplied data_size is cast to signed int before being used in min_t(). Large unsigned values (>= 0x80000000) become negative, causing unsigned wraparound and oversized memcpy operations that can overflow the stack buffer. Change min_t(int, ...) to min() as both values are unsigned and can be handled by min() without explicit cast.	2026-06-25	7.8	CVE-2026-53202
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/ivpu: Add buffer overflow check in MS get_info_ioctl Add validation that the info size returned from the metric stream info query is not exceeded when checked against the allocated buffer size. If the firmware returns a size larger than the buffer, reject the operation with -EOVERFLOW instead of proceeding with an incorrect buffer copy.	2026-06-25	7.1	CVE-2026-53203
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: accel/ivpu: Add bounds checks for firmware log indices Add validation that read and write indices in the firmware log buffer are within valid bounds (< data_size) before using them. If out-of-bounds indices are encountered (from firmware), clamp them to safe values instead of proceeding with invalid offsets. This prevents potential out-of-bounds buffer access when firmware supplies invalid log indices.	2026-06-25	7.1	CVE-2026-53205
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: reject oversized Broadcast Announcement prepend Existing advertising instances can already hold the maximum extended advertising payload. When hci_adv_bcast_announcement() prepends the Broadcast Announcement service data to that payload, the combined data may no longer fit in the temporary buffer used to rebuild the advertising data. Reject that case before copying the existing payload and report the failure through the device log. This keeps the existing advertising data intact and avoids overrunning the temporary buffer.	2026-06-25	7.8	CVE-2026-53209
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_tunnel: fix use-after-free on object destroy nft_tunnel_obj_destroy() calls metadata_dst_free() which directly kfree()s the metadata_dst, ignoring the dst_entry refcount. Packets that took a reference via dst_hold() in nft_tunnel_obj_eval() and are still queued (e.g. in a netem qdisc) are left with a dangling pointer. When these packets are eventually dequeued, dst_release() operates on freed memory. Replace metadata_dst_free() with dst_release() so the metadata_dst is freed only after all references are dropped. The dst subsystem already handles metadata_dst cleanup in dst_destroy() when DST_METADATA is set.	2026-06-25	7.8	CVE-2026-53212
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: guard timestamp cmsgs to real error queue skbs skb_is_err_queue() treats PACKET_OUTGOING as the sole marker for an skb from sk_error_queue. That assumption is not true for AF_PACKET sockets: outgoing packet taps are also delivered to packet sockets with skb->pkt_type == PACKET_OUTGOING, but their skb->cb is owned by AF_PACKET instead of struct sock_exterr_skb. If such an skb is received with timestamping	2026-06-25	7.1	CVE-2026-53223

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	enabled, the generic timestamp cmsg path can read AF_PACKET control-buffer state as sock_exterr_skb::opt_stats. With SO_RXQ_OVFL enabled, the packet drop counter overlaps opt_stats. An odd drop count makes the path emit SCM_TIMESTAMPING_OPT_STATS with skb->len and skb->data. For non-linear skbs this copies past the linear head and can trigger hardened usercopy or disclose adjacent heap contents. Keep skb_is_err_queue() local to net/socket.c, but make it verify that the PACKET_OUTGOING marker is paired with the sock_rmem_free destructor installed by sock_queue_err_skb(). AF_PACKET receive skbs use normal receive ownership and no longer pass as error-queue skbs, while legitimate sk_error_queue entries keep the PACKET_OUTGOING marker and sock_rmem_free ownership.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: xsk: Fix DMA and xdp_frame leak on XDP_TX xmit failure In the XSK branch of mlx5e_xmit_xdp_buff(), when sq->xmit_xdp_frame() returns false (e.g. XDPSQ is full), the function returns without unmapping the DMA address or freeing the xdp_frame allocated by xdp_convert_zc_to_xdp_frame(). The xdpi_fifo push only happens on success, so the completion path cannot recover these entries. With CONFIG_DMA_API_DEBUG=y, the leak surfaces on driver unbind: DMA-API: pci 0000:08:00:0: device driver has pending DMA allocations while released from device [count=1116] One of leaked entries details: [device address=0x000000010ffd7028] [size=1534 bytes] [mapped with DMA_TO_DEVICE] [mapped as phy] WARNING: kernel/dma/debug.c:881 at dma_debug_device_change+0x127/0x180 ... DMA-API: Mapped at: debug_dma_map_phys+0x4b/0xd0 dma_map_phys+0xfd/0x2d0 mlx5e_xdp_handle+0x5ae/0xac0 [mlx5_core] mlx5e_xsk_skb_from_cqe_mpwrq_linear+0xc4/0x170 [mlx5_core] mlx5e_handle_rx_cqe_mpwrq+0xc1/0x290 [mlx5_core] Add the missing unmap + xdp_return_frame, matching the cleanup already done in mlx5e_xdp_xmit(). has_frags is rejected earlier in this branch, so no per-frag unmap is needed.	2026-06-25	7.5	CVE-2026-53229
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: add pskb_may_pull() to skb_gro_receive_list() skb_gro_receive_list() calls skb_pull(skb, skb_gro_offset(skb)) without first ensuring the data is in the linear area via pskb_may_pull(). When the skb arrives via napi_gro_frags(), skb_headlen can be 0 (all data in page fragments) while skb_gro_offset is non-zero (after IP+TCP header parsing). The skb_pull() then decrements skb->len by skb_gro_offset but skb->data_len stays unchanged, hitting BUG_ON(skb->len < skb->data_len) in __skb_pull(). The UDP fraglist GRO path already contains this guard at udp_offload.c:749. Adding it to skb_gro_receive_list() itself provides centralized protection for all callers (TCP, UDP, and any future protocols), and ensures the precondition of skb_pull() is satisfied before it is called. On pskb_may_pull() failure, set NAPI_GRO_CB(skb)->flush = 1 so the skb is not held as a new GRO head and is instead delivered through the normal receive path, matching the UDP handling.	2026-06-25	7.5	CVE-2026-53235
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: policy: fix use-after-free on inexact bin in xfrm_policy_byysel_ctx() Fix the race by pruning the bin while still holding xfrm_policy_lock, before dropping it. Use __xfrm_policy_inexact_prune_bin() directly since the lock is already held. The wrapper xfrm_policy_inexact_prune_bin() becomes unused and is removed. Race: CPU0 (XFRM_MSG_DELPOLICY) CPU1 (XFRM_MSG_NEWSPDINFO) ===== xfrm_policy_byysel_ctx(): spin_lock_bh(xfrm_policy_lock) bin = xfrm_policy_inexact_lookup() __xfrm_policy_unlink(pol) spin_unlock_bh(xfrm_policy_lock) xfrm_policy_kill(ret) // wide window, lock not held xfrm_hash_rebuild(): spin_lock_bh(xfrm_policy_lock) __xfrm_policy_inexact_flush():	2026-06-25	7.8	CVE-2026-53239

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	kfree_rcu(bin) // bin freed spin_unlock_bh(xfrm_policy_lock) xfrm_policy_inexact_prune_bin(bin) // UAF: bin is freed			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: PCM: Fix wait queue list corruption in snd_pcm_drain() on linked streams snd_pcm_drain() uses init_waitqueue_entry which does not clear entry.prev/next, and add_wait_queue with a conditional remove_wait_queue that is skipped when to_check is no longer in the group after concurrent UNLINK. The orphaned wait entry remains on the unlinked substream sleep queue. On the next drain iteration, add_wait_queue adds the entry to a new queue while still linked on the old one, corrupting both lists. A subsequent wake_up dereferences NULL at the func pointer (mapped from the spinlock at offset 0 of the misinterpreted wait_queue_head_t), causing a kernel panic. Replace init_waitqueue_entry/add_wait_queue/conditional remove_wait_queue with init_wait_entry/prepare_to_wait/ finish_wait. init_wait_entry clears prev/next via INIT_LIST_HEAD on each iteration and sets autoremove_wake_function which auto-removes the entry on wake-up. finish_wait safely handles both the already-removed and still-queued cases.	2026-06-25	7.8	CVE-2026-53242
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: VFS: fix possible failure to unlock in nfsd4_create_file() atomic_create() in fs/namei.c drops the reference to the dentry when it returns an error. This behaviour was imported into dentry_create() so that it will drop the reference if an error is returned from atomic_create(), though not if vfs_create() returns an error (in the case where ->atomic_create is not supported). The caller - nfsd4_create_file() - is made aware of this by checking path->dentry, which will either be a counted reference to a dentry, or an error pointer. However the change to use start_creating()/end_creating() (which landed shortly before the dentry_create() change landed, though was likely developed around the same time) means that nfsd4_create_file() *needs* a valid dentry so that it can unlock the parent. The net result is that if NFSD exports a filesystem which uses ->atomic_create, and if a call to ->atomic_create returns an error, then nfsd4_create_file() will pass an error pointer to end_creating() and the parent will not be unlocked. Fix this by changing dentry_create() to make sure path->dentry is always a valid dentry, never an error-pointer. The actual error is already returned a different way. Note that if ->atomic_create() returns a different dentry (which may not be possible in practice) we are guaranteed (because it is only ever provided by d_splince_alias()) that it will have the same d_parent and so it will have the same effect when passed to end_creating().	2026-06-25	7.5	CVE-2026-53244
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: xsk: cache csum_start/csum_offset to fix TOCTOU in xsk_skb_metadata() The TX metadata area resides in the UMEM buffer which is memory-mapped and concurrently writable by userspace. In xsk_skb_metadata(), csum_start and csum_offset are read from shared memory for bounds validation, then read again for skb assignment. A malicious userspace application can race to overwrite these values between the two reads, bypassing the bounds check and causing out-of-bounds memory access during checksum computation in the transmit path. Fix this by reading csum_start and csum_offset into local variables once, then using the local copies for both validation and assignment. Note that other metadata fields (flags, launch_time) and the cached csum fields may be mutually inconsistent due to concurrent userspace writes, but this is benign: the only security-critical invariant is that each field's validated value is the same one used, which local caching guarantees.	2026-06-25	7.8	CVE-2026-53250
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: bnep: reject short frames before parsing A BNEP peer can send a short BNEP SDU. bnep_rx_frame() reads the packet type byte	2026-06-25	7.1	CVE-2026-53253

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	immediately and, for control packets, reads the control opcode and setup UUID-size byte before proving that those bytes are present. bnep_rx_control() also dereferences the control opcode without rejecting an empty control payload. Use skb_pull_data() for the fixed fields in bnep_rx_frame() so a NULL return gates each dereference. Split the control handler so the frame path can pass an opcode that has already been pulled, and keep the byte-buffer wrapper for extension control payloads. For BNEP_SETUP_CONN_REQ, name the UUID-size byte before pulling the setup payload. struct bnep_setup_conn_req carries destination and source service UUIDs after that byte, each uuid_size bytes, so the parser now documents that tuple explicitly instead of leaving the pull length as an opaque multiplication. Validation reproduced this kernel report: KASAN slab-out-of-bounds in bnep_rx_frame.isra.0+0x130c/0x1790 The buggy address belongs to the object at ffff88800c0f7908 which belongs to the cache kmalloc-8 of size 8 The buggy address is located 0 bytes to the right of allocated 1-byte region [ffff88800c0f7908, ffff88800c0f7909) Read of size 1 Call trace: dump_stack_lvl+0xb3/0x140 (?:?) print_address_description+0x57/0x3a0 (?:?) bnep_rx_frame+0x130c/0x1790 (net/bluetooth/bnep/core.c:306) print_report+0xb9/0x2b0 (?:?) __virt_addr_valid+0x1ba/0x3a0 (?:?) srso_alias_return_thunk+0x5/0xfbef5 (?:?) kasan_addr_to_slab+0x21/0x60 (?:?) kasan_report+0xe0/0x110 (?:?) process_one_work+0xfce/0x17e0 (kernel/workqueue.c:3200) worker_thread+0x65c/0xe40 (?:?) __kthread_parkme+0x184/0x230 (?:?) kthread+0x35e/0x470 (?:?) _raw_spin_unlock_irq+0x28/0x50 (?:?) ret_from_fork+0x586/0x870 (?:?) __switch_to+0x74f/0xdc0 (?:?) ret_from_fork_asm+0x1a/0x30 (?:?)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: anycast: insert aca into global hash under idev->lock syzbot reported a splat [1]: a slab-use-after-free in ipv6_chk_acast_addr(), which walks the global inet6_acaddr_lst[] hash under RCU and dereferences a struct ifacaddr6 that has already been freed while still linked in the hash, so a later reader walks into a dangling node. In __ipv6_dev_ac_inc() the aca is allocated with refcount 1, then aca_get() bumps it to 2 to keep it alive across the unlocked region. It is published to idev->ac_list under idev->lock, but ipv6_add_acaddr_hash() runs after write_unlock_bh(). A concurrent teardown (ipv6_ac_destroy_dev() from addrconf_ifdown(), under RTNL) can slip into that window: CPU0 __ipv6_dev_ac_inc CPU1 ipv6_ac_destroy_dev (RTNL) ----- ----- aca_alloc() refcnt 1 aca_get() refcnt 2 write_lock_bh(idev->lock) add aca to ac_list write_unlock_bh(idev->lock) write_lock_bh(idev->lock) pull aca off ac_list write_unlock_bh(idev->lock) ipv6_del_acaddr_hash(aca) hlist_del_init_rcu() is a no-op, aca is not in the hash yet aca_put() refcnt 2->1 ipv6_add_acaddr_hash(aca) aca now inserted into the hash aca_put() refcnt 1->0 call_rcu(aca_free_rcu) -> kfree(aca) The hash removal becomes a no-op because the insertion has not happened yet, so once CPU0 inserts and drops the last reference, the aca is freed while still linked in inet6_acaddr_lst[], and readers dereference freed memory after the slab slot is reused. This window opened once RTNL stopped serializing the join path against device teardown. Move ipv6_add_acaddr_hash() inside the idev->lock section so the ac_list and hash insertions are atomic with respect to teardown: a racing remover now either misses the aca entirely or finds it in both lists. acaddr_hash_lock is now nested under idev->lock, which is acquired in softirq context, so switch all acaddr_hash_lock sites to spin_lock_bh() to avoid the irq lock inversion reported in [2]. [1] https://syzkaller.appspot.com/bug?extid=a01df04303c131efbf3a [2] https://lore.kernel.org/netdev/6a194ef7.ba3b1513.1890b4.0000.GAE@google.com/	2026-06-25	7.8	CVE-2026-53259

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: l2tp: pppol2tp: hold reference to session in pppol2tp_ioctl() pppol2tp_ioctl() read sock->sk->sk_user_data directly without any locks or reference counting. If a controllable sleep was induced during copy_from_user() (e.g. via a userfaultfd page fault sleep), a concurrent socket close could trigger pppol2tp_session_close() asynchronously. This frees the l2tp_session structure via the l2tp_session_del_work workqueue. Upon resuming, the ioctl thread dereferences the stale session pointer, resulting in a Use-After-Free (UAF). Fix this by securely fetching the session reference using the RCU-safe, refcounted helper pppol2tp_sock_to_session(sk) on entry. This locks the session's refcount across the sleep. We structured the function to exit via standard err breaks, guaranteeing that l2tp_session_put() is cleanly called on all return paths to drop the reference. To preserve existing behavior we validate the session and its magic signature only for the specific L2TP commands that require it. This ensures that generic/unknown ioctls called on an unconnected socket still return -ENOIOCTLCMD and correctly fall back to generic handlers (e.g. in sock_do_ioctl()).	2026-06-25	7.8	CVE-2026-53262
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_api: use RCU with deferred freeing for action lifecycle When NEWTFILTER and DELFILTER are run concurrently it is possible to create a race with an associated action. Let's illustrate with CPU0 running NEWTFILTER and CPU1 running DELFILTER: 0: mutex_lock() <-- holds the idr lock 0: rcu_read_lock() 0: p = idr_find(idr, index) <-- action p is valid (RCU protects IDR) 0: mutex_unlock() <-- releases the idr lock 1: refcount_dec_and_mutex_lock() <-- refcnt 1->0, mutex held 1: idr_remove(idr, index) <-- Action removed from IDR 1: mutex_unlock() <-- mutex released allowing us to delete the action 1: tcf_action_cleanup(p); kfree(p) <-- Kfree's p immediately, no deferral 0: refcount_inc_not_zero(&p->tcfa_refcnt) <-- ouch, UAF p points to freed memory This patch fixes the race condition between NEWTFILTER and DELFILTER by adding struct rcu_head to tc_action used in the deferral and introducing a call_rcu() in the delete path to defer the final kfree(). Note: this is a revert of commit d7fb60b9cafb ("net_sched: get rid of tcfa_rcu") but also modernization/simplification to directly use kfree_rcu(). Let's illustrate the new restored code path: 0: rcu_read_lock() 1: refcount_dec_and_mutex_lock() <-- refcnt 1->0, mutex held 1: idr_remove(idr, index) 1: mutex_unlock() 1: call_rcu(&p->tcfa_rcu, tcf_action_rcu_free) <-- defer kfree after grace period 0: p = idr_find(idr, index) 0: refcount_inc_not_zero(&p->tcfa_refcnt) <-- fails, refcnt already 0 1: rcu_read_unlock() <-- release so freeing can run after grace period After CPU1 calls idr_remove(), the object is no longer reachable through the IDR. CPU0's subsequent idr_find() will return NULL, and even if it still held a stale pointer, the immediate kfree() is now deferred until after the RCU grace period, so no UAF can occur.	2026-06-25	7.8	CVE-2026-53264
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: dm cache policy smq: check allocation under invalidate lock commit 2d1f7b65f5de ("dm cache policy smq: fix missing locks in invalidating cache blocks") added mq->lock around the destructive part of smq_invalidate_mapping(), but left the e->allocated check outside the critical section. That leaves a check-then-act race. Two concurrent invalidators can both observe e->allocated as true before either of them takes mq->lock. The first invalidator that acquires the lock removes the entry from the queues and hash table and then calls free_entry(), which clears e->allocated and puts the entry back on the free list. The second invalidator can then acquire mq->lock and continue with the stale result of the unlocked check. This can corrupt the SMQ queues or hash table by deleting an entry that is no longer on those structures. It can also hit the allocation check in free_entry() when the same entry is freed again. Move	2026-06-25	7.8	CVE-2026-53265

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the allocation check under mq->lock so the predicate and the destructive operations are serialized by the same lock.			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_ct: bail out on template ct in get eval I noticed this issue while looking at a historic syzbot report [1]. A rule like the one below is enough to trigger the bug: table ip t { chain pre { type filter hook prerouting priority raw; ct zone set 1 ct original saddr 1.2.3.4 accept } } The first expression attaches a per-cpu template ct via nft_ct_set_zone_eval() (nf_ct_tmpl_alloc -> kzalloc, tuple is all zero, nf_ct_l3num(ct) == 0). The next expression then calls nft_ct_get_eval() on the same skb, treats the template as a real ct and hits the 16-byte memcpy path. With dreg at NFT_REG32_15 this overflows past struct nft_regs on the kernel stack; with smaller dreg values it silently clobbers adjacent registers. Reject template ct at the eval entry and in nft_ct_get_fast_eval(), mirroring the check nft_ct_set_eval() already has. Additionally, bound the address copy in NFT_CT_SRC / NFT_CT_DST by priv->len instead of by nf_ct_l3num(ct): nf_ct_get_tuple() zeroes the tuple before pkt_to_tuple() fills in only the protocol-relevant leading bytes, so the trailing bytes of tuple->{src,dst}.u3.all are well-defined zero. priv->len is validated at rule load, so the copy size is now bounded by the destination register rather than by an untrusted field on the conntrack. [1]: https://syzkaller.appspot.com/bug?id=389cf09cb72926114fce90dc85a2c3231dcb647c	2026-06-25	7.8	CVE-2026-53267
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: clear the svc scheduler ptr early on edit ip_vs_edit_service() while unbinding the old scheduler clears the svc->scheduler ptr after the scheduler module initiates RCU callbacks. This can cause packets to use the old scheduler at the time when svc->sched_data is already freed after RCU grace period. Fix it by clearing the ptr early in ip_vs_unbind_scheduler(), before the done_service method schedules any RCU callbacks. Also, if the new scheduler fails to initialize when replacing the old scheduler, try to restore the old scheduler while still returning the error code.	2026-06-25	7.8	CVE-2026-53270
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: tee: optee: prevent use-after-free when the client exits before the supplicant Commit 70b0d6b0a199 ("tee: optee: Fix supplicant wait loop") made the client wait as killable so it can be interrupted during shutdown or after a supplicant crash. This changes the original lifetime expectations: the client task can now terminate while the supplicant is still processing its request. If the client exits first it removes the request from its queue and kfree()s it, while the request ID remains in supp->idr. A subsequent lookup on the supplicant path then dereferences freed memory, leading to a use-after-free. Serialise access to the request with supp->mutex: * Hold supp->mutex in optee_supp_recv() and optee_supp_send() while looking up and touching the request. * Let optee_supp_thrd_req() notice that the client has terminated and signal optee_supp_send() accordingly. With these changes the request cannot be freed while the supplicant still has a reference, eliminating the race.	2026-06-25	7.8	CVE-2026-53273
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: Fix a use-after-free of the hci_conn pointer In iso_sock_rebind_bc(), the bis pointer is cached, then the socket lock is dropped: bis = iso_pi(sk)->conn->hcon; /* Release the socket before lookups since that requires hci_dev_lock * which shall not be acquired while holding sock_lock for proper * ordering. */ release_sock(sk); hci_dev_lock(bis->hdev); During the unlocked window, could a concurrent close() destroy the connection and free the bis structure, causing hci_dev_lock(bis->hdev) to access memory after it is freed, fix this by using the hdev reference which was safely acquired via iso_conn_get_hdev().	2026-06-25	7.8	CVE-2026-53276
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: only release the dirty pages io tree after successful writes [WARNING]	2026-06-26	7.5	CVE-2026-53284

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	With extra warning on dirty extent buffers at umount (aka, the next patch in the series), test case generic/388 can trigger the following warning about dirty extent buffers at unmount time: BTRFS critical (device dm-2 state E): emergency shutdown BTRFS error (device dm-2 state E): error while writing out transaction: -30 BTRFS warning (device dm-2 state E): Skipping commit of aborted transaction. BTRFS error (device dm-2 state EA): Transaction 9 aborted (error -30) BTRFS: error (device dm-2 state EA) in cleanup_transaction:2068: errno=-30 Readonly filesystem BTRFS info (device dm-2 state EA): forced readonly BTRFS info (device dm-2 state EA): last unmount of filesystem 4fbf2e15-f941-49a0-bc7c-716315d2777c ----- ---[cut here]----- WARNING: disk-io.c:3311 at invalidate_and_check_btree_folios+0xfd/0x1ca [btrfs], CPU#8: umount/914368 CPU: 8 UID: 0 PID: 914368 Comm: umount Tainted: G OE 7.1.0-rc1-custom+ #372 PREEMPT(full) 2de38db8d1deae71fde295430a0ff3ab98ccf596 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS unknown 02/02/2022 RIP: 0010:invalidate_and_check_btree_folios+0xfd/0x1ca [btrfs] Call Trace: <TASK> close_ctree+0x52e/0x574 [btrfs] d2f0b1cd330d1287e7a9919d112eadfc0e914efd] generic_shutdown_super+0x89/0x1a0 kill_anon_super+0x16/0x40 btrfs_kill_super+0x16/0x20 [btrfs] d2f0b1cd330d1287e7a9919d112eadfc0e914efd] deactivate_locked_super+0x2d/0xb0 cleanup_mnt+0xdc/0x140 task_work_run+0x5a/0xa0 exit_to_user_mode_loop+0x123/0x4b0 do_syscall_64+0x243/0x7c0 entry_SYSCALL_64_after_hwframe+0x4b/0x53 </TASK> ---[end trace 0000000000000000]--- BTRFS warning (device dm-2 state EA): unable to release extent buffer 30539776 owner 9 gen 9 refs 2 flags 0x7 BTRFS warning (device dm-2 state EA): unable to release extent buffer 30621696 owner 257 gen 9 refs 2 flags 0x7 BTRFS warning (device dm-2 state EA): unable to release extent buffer 30638080 owner 258 gen 9 refs 2 flags 0x7 BTRFS warning (device dm-2 state EA): unable to release extent buffer 30654464 owner 7 gen 9 refs 2 flags 0x7 BTRFS warning (device dm-2 state EA): unable to release extent buffer 30703616 owner 2 gen 9 refs 2 flags 0x7 BTRFS warning (device dm-2 state EA): unable to release extent buffer 30720000 owner 10 gen 9 refs 2 flags 0x7 BTRFS warning (device dm-2 state EA): unable to release extent buffer 30736384 owner 4 gen 9 refs 2 flags 0x7 BTRFS warning (device dm-2 state EA): unable to release extent buffer 30752768 owner 11 gen 9 refs 2 flags 0x7 I'm using a stripped down version, which seems to trigger the warning more reliably: _fsstress_pid="" workload() { dmesg -C mkfs.btrfs -f -K \$dev > /dev/null echo 1 > /sys/kernel/debug/clear_warn_once mount \$dev \$mnt \$fsstress -w -n 1024 -p 4 -d \$mnt & _fsstress_pid=\$! sleep 0 \$godown \$mnt pkill --echo -PIPE fsstress > /dev/null wait \$ _fsstress_pid unset _fsstress_pid umount \$mnt if dmesg grep -q "WARNING"; then fail fi } for ((i = 0; i < \$runtime; i++)); do echo "=== \$i/\$runtime ===" workload done [CAUSE] Inside btrfs_write_and_wait_transaction(), we first try to write all dirty ebs, then wait for them to finish. After that we call btrfs_extent_io_tree_release() to free all extent states from dirty_pages io tree. However if we hit an error from btrfs_write_marked_extent(), then we still call btrfs_extent_io_tree_release() to clear that dirty_pages io tree, which may contain dirty records that we haven't yet submitted. Furthermore, the later transaction cleanup path will utilize that dirty_pages io tree to properly cleanup those dirty ebs, but since it's already empty, no dirty ebs are properly cleaned up, thus will later trigger the warnings inside invalidate_btree_folios(). ---truncated---			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/eustall: Fix drm_dev_put called before stream disable in close In xe_eu_stall_stream_close(), drm_dev_put() is called before the stream is	2026-06-26	7.8	CVE-2026-53290

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	disabled and its resources are freed. If this drops the last reference, the device structures could be freed while the subsequent cleanup code still accesses them, leading to a use-after-free. Fix this by moving <code>drm_dev_put()</code> after all device accesses are complete. This matches the ordering in <code>xe_oa_release()</code> . (cherry picked from commit 35aff528f7297e949e5e19c9cd7fd748cf1cf21c)			
Linux--Linux	In the Linux kernel, the following vulnerability has been resolved: net: enetc: fix NTMP DMA use-after-free issue The AI-generated review reported a potential DMA use-after-free issue [1]. If <code>netc_xmit_ntmp_cmd()</code> times out and returns an error, the pending command is not explicitly aborted, while <code>ntmp_free_data_mem()</code> unconditionally frees the DMA buffer. If the buffer has already been reallocated elsewhere, this may lead to silent memory corruption. Because the hardware eventually processes the pending command and perform a DMA write of the response to the physical address of the freed buffer. To resolve this issue, this patch does the following modifications: 1. Convert <code>cbdr->ring_lock</code> from a spinlock to a mutex The lock was originally a spinlock in case NTMP operations might be invoked from atomic context. After downstream support for all NTMP tables, no such usage has materialized. A mutex lock is now required because the driver now needs to reclaim used BDs and release associated DMA memory within the lock's context, while <code>dma_free_coherent()</code> might sleep. 2. Introduce software command BD (struct <code>netc_swcbd</code>) The hardware write-back overwrites the <code>addr</code> and <code>len</code> fields of the BD, so the driver cannot rely on the hardware BD to free the associated DMA memory. The driver now maintains a software shadow BD storing the DMA buffer pointer, DMA address, and size. And <code>netc_xmit_ntmp_cmd()</code> only reclaims older BDs when the number of used BDs reaches <code>NETC_CBDR_CLEAN_WORK</code> (16). The software BD enables correct DMA memory release. With this, struct <code>ntmp_dma_buf</code> and <code>ntmp_free_data_mem()</code> are no longer needed and are removed. 3. Require callers to hold <code>ring_lock</code> across <code>netc_xmit_ntmp_cmd()</code> <code>netc_xmit_ntmp_cmd()</code> releases the <code>ring_lock</code> before the caller finishes consuming the response. At this point, if a concurrent thread submits a new command, it may trigger <code>ntmp_clean_cbdr()</code> and free the DMA buffer while it is still in use. Move <code>ring_lock</code> ownership to the caller to ensure the response buffer cannot be reclaimed prematurely. So the helpers <code>ntmp_select_and_lock_cbdr()</code> and <code>ntmp_unlock_cbdr()</code> are added. These changes eliminate the DMA use-after-free condition and ensure safe and consistent BD reclamation and DMA buffer lifecycle management.	2026-06-26	7.8	CVE-2026-53300
ljharb--shell-quote	shell-quote prior to 1.8.5 finalizes parsed tokens in <code>parse()</code> using <code>Array.prototype.concat</code> as a reduce accumulator, which reallocates and copies the entire growing array on every iteration. As a result <code>parse()</code> runs in $O(n^2)$ time relative to the number of input tokens. An attacker who can supply an attacker-controlled string to any code path that calls <code>parse()</code> (no shell metacharacters are required; plain space-separated words suffice) can block the single-threaded Node.js event loop for an extended period with a small input, resulting in a denial of service. There is no code execution or data disclosure; impact is to availability only. Fixed in 1.8.5.	2026-06-25	7.5	CVE-2026-13311
lobehub--lobehub	LobeHub is a work-and-lifestyle space to find, build, and collaborate with agent teammates that grow with you. Prior to 2.1.57, the <code>/webapi/proxy</code> endpoint on <code>app.lobehub.com</code> accepts a URL in the POST body and fetches it server-side without any authentication. An attacker can use this to make arbitrary outbound requests from LobeHub's infrastructure, leak Vercel deployment details, and inject cookies on the <code>lobehub.com</code> domain through reflected Set-Cookie headers. This vulnerability is fixed in 2.1.57.	2026-06-23	9	CVE-2026-54157
lostisland--faraday	Faraday is an HTTP client library abstraction layer that provides a common interface over many adapters. From 1.0.0 until 1.10.6 and 2.14.3, <code>Faraday::NestedParamsEncoder</code> , the default nested query parameter encoder/decoder in Faraday, decodes nested query strings without	2026-06-24	7.5	CVE-2026-54297

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	enforcing a maximum nesting depth. A crafted query string causes Faraday to build a deeply nested Ruby Hash structure. The internal dehesh routine then recursively walks this attacker-controlled structure without a depth limit. At sufficient depth, Ruby raises an uncaught SystemStackError (stack level too deep), crashing the calling thread or worker. This can lead to denial of service in applications that pass attacker-controlled query strings to Faraday's nested query parsing or URL-building paths. This vulnerability is fixed in 1.10.6 and 2.14.3.			
MainWP--MainWP Child	Unauthenticated Broken Access Control in MainWP Child <= 6.1.1 versions.	2026-06-25	7.5	CVE-2026-27366
MarketingFire--Widget Options	Contributor Remote Code Execution (RCE) in Widget Options <= 4.2.3 versions.	2026-06-25	9.9	CVE-2026-54823
MarlinFirmware--Marlin	Marlin Firmware through 2.1.2.7, fixed in commit 1f255d1, when built with MESH_BED_LEVELING enabled, contains an out-of-bounds write vulnerability in the M421 G-code handler that allows attackers to corrupt firmware memory by supplying out-of-range X and Y grid indices. Attackers can send a single crafted G-code command via USB serial, network interface, or malicious gcode file to write an attacker-controlled 32-bit float value past the z_values array bounds, corrupting adjacent firmware variables and causing denial of service or firmware state corruption.	2026-06-24	9.1	CVE-2026-56111
mastodon--mastodon	Mastodon is a free, open-source social network server based on ActivityPub. Prior to 4.5.10, 4.4.17, and 4.3.23, when using Ruby versions older than 3.4, PrivateAddressCheck.private_address? returns false for IPv4-mapped IPv6 addresses (::ffff:a.b.c.d) corresponding to some private IPv4 addresses, depending on Ruby version, this can include loopback, RFC1918 private networks, and link-local space. An attacker who controls DNS for any domain can publish an AAAA record with such a mapped address; any outbound HTTP fetch Mastodon performs against that hostname then opens a real TCP connection to the underlying IPv4 address, including 127.0.0.1 and cloud-metadata endpoints such as 169.254.169.254. This vulnerability is fixed in 4.5.10, 4.4.17, and 4.3.23.	2026-06-24	8.6	CVE-2026-47389
mastodon--mastodon	Mastodon is a free, open-source social network server based on ActivityPub. Prior to 4.5.11, 4.4.18, and 4.3.24, a DoS can be triggered by (Uncaught Exception vulnerability), due to missing exception handling in the math sanitizer. Malformed <math> nodes can result in a DoS of a whole server or targeted users services, depending on the type of action that includes the malformed nodes and the services interacting with it. This vulnerability is fixed in 4.5.11, 4.4.18, and 4.3.24.	2026-06-24	7.5	CVE-2026-50129
max-mapper--extract-zip	extract-zip does not validate symlink targets when extracting zip archives. When processing a malicious zip file containing a symlink with a relative path like '.././.././etc/passwd', extract-zip will extract the symlink without validation, allowing it to point outside the extraction directory. Depending on how extract-zip is used, an attacker could read or write to arbitrary files.	2026-06-26	8.1	CVE-2026-56876
MB connect line--mbCONNECT24	An high privileged remote attacker can access a hidden configuration method, that should not be accessible by any user, to modify critical program parameters. This can result in a total loss of confidentiality, integrity and availability.	2026-06-23	7.2	CVE-2026-10521
Melapress--WP Activity Log	Subscriber Cross Site Scripting (XSS) in WP Activity Log <= 5.6.3.1 versions.	2026-06-25	7.1	CVE-2026-56005
MessagePack-CSharp--MessagePack-CSharp	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, A vulnerability exists in the optional LZ4 decompression path used by MessagePack compression modes Lz4Block and Lz4BlockArray. The decoder implementation is based on a deprecated fast-decompression algorithm that does not take a source-length bound. A remote attacker can send a crafted MessagePack payload with manipulated LZ4 token/length fields to force out-of-bounds reads from the compressed input buffer. In affected environments, this can trigger an AccessViolationException during decompression, causing process	2026-06-22	8.2	CVE-2026-48109

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	termination (denial of service). Under some conditions, limited unintended memory disclosure from over-read data may also be possible before failure. This vulnerability is fixed in 2.5.301 and 3.1.7.			
MessagePack-CSharp-- MessagePack-CSharp	MessagePack for C# is a MessagePack serializer for C#. Prior to 2.5.301 and 3.1.7, MessagePackReader.TrySkip() recursively descends into nested arrays and maps without incrementing the reader depth or calling the configured depth checks. This bypasses MessagePackSecurity.MaximumObjectGraphDepth, the library's documented protection against deeply nested object graphs. Many generated and dynamic formatters call reader.Skip() when they encounter unknown map keys, unknown array members, ignored fields, or data that should be skipped for forward compatibility. A deeply nested value in one of these skipped positions can therefore cause unbounded recursion and an uncatchable StackOverflowException. This vulnerability is fixed in 2.5.301 and 3.1.7.	2026-06-22	7.5	CVE-2026-48506
MHSanaei--3x-ui	3X-UI is a web control panel for managing Xray-core servers. Prior to 3.3.1, an authenticated administrator can abuse the database import functionality to achieve arbitrary file write on the host by modifying Xray configuration values stored in the database. This can be leveraged to obtain code execution and persistent access as the user running Xray (including root when Xray is running as root). This vulnerability is fixed in 3.3.1.	2026-06-25	7.2	CVE-2026-55477
miurahr--py7zr	py7zr is a Python-based library and utility to support 7zip archive compression, decompression, encryption and decryption. Versions 1.1.2 and below contain an arbitrary file write vulnerability, which allows symbolic links to be recreated outside the destination directory via crafted malicious symbolic link chains. When using extractall to extract an archive, the library restores these symbolic links, linking them to arbitrary directories on the host file system. During extraction, the program only checks the link arcname within the destination directory, but ignores the combined symlink path resolution. Attackers can exploit this vulnerability by constructing malicious archives, thereby bypassing the directory boundary restrictions implemented by the extractor. Subsequent extraction of regular files through these symbolic links can result in arbitrary file writes. This vulnerability may lead to remote code execution, privilege escalation, data corruption, or denial of service. This issue has been fixed in version 1.1.3.	2026-06-24	8	CVE-2026-23879
MyBB--MyBB	MyBB 1.8.40 does not restrict which usergroup a limited Admin Control Panel user may assign when creating or editing users; the user module offers the Administrators group (gid 4) and its datahandler's verify_usergroup() unconditionally returns true. An admin holding only the delegated user-management permission can assign the Administrators group to an account and escalate to the full Administrator permission set.	2026-06-28	7.2	CVE-2026-58054
n8n--n8n	n8n before 2.20.0 contains a credential exfiltration vulnerability in the POST /rest/dynamic-node-parameters/options endpoint that allows authenticated users to bypass Allowed HTTP Request Domains restrictions. Attackers with credential access can cause the n8n server to issue HTTP requests with credentials to unauthorized hosts, exfiltrating sensitive authentication data.	2026-06-22	9.1	CVE-2026-56348
n8n--n8n	n8n before version 2.4.0 contains a sql injection vulnerability in MySQL, PostgreSQL, and Microsoft SQL nodes that allows authenticated users to inject arbitrary SQL through unescaped identifier values in node configuration parameters. Attackers with workflow creation permissions can supply specially crafted table or column names to execute unauthorized database commands and compromise data integrity.	2026-06-24	8.2	CVE-2026-56351
NetComm Wireless Pty Ltd--NF20MESH	NetComm NF20MESH routers running firmware R6B031 and earlier contain an authenticated remote code execution vulnerability that allows authenticated attackers to execute arbitrary commands as root by injecting shell metacharacters into the username JSON parameter	2026-06-23	8.8	CVE-2026-35018

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	processed by the dalStorage_addUserAccount function. Attackers can exploit the unsafe concatenation of user-supplied input into a shell command string passed to rut_doSystemAction without sanitization to achieve full root-level command execution on the underlying operating system.			
NetComm Wireless Pty Ltd--NF20MESH	NetComm NF20MESH routers running firmware R6B031 and earlier contain an authentication bypass vulnerability that allows unauthenticated attackers to gain administrative access by exploiting a hardcoded AES-256 key used to encrypt session cookies for the web management interface. Attackers can forge a valid encrypted session cookie using the shared hardcoded key and bypass authentication checks to obtain full administrative control of the management interface while any legitimate administrator session is active.	2026-06-23	8.1	CVE-2026-35019
newscred--Welcome Software Publishing	The Welcome Software Publishing plugin for WordPress is vulnerable to Arbitrary Options Update in all versions up to and including 0.0.31. This is due to a missing capability check in the nc_setOption() function, which is exposed via the nc.setOption XML-RPC method. The function authenticates the user via \$wp_xmlrpc_server->login() (verifying credentials are valid) but does not perform any authorization check such as current_user_can('manage_options'). This makes it possible for authenticated attackers, with Subscriber-level access and above, to update arbitrary WordPress options via XML-RPC requests. This can be leveraged to change the default_role option to 'administrator' and then register a new administrator account, achieving full privilege escalation and site takeover.	2026-06-24	8.8	CVE-2026-4297
nicashmu--Cincopa video and media plug-in	The Cincopa video and media plug-in plugin for WordPress is vulnerable to Stored Cross-Site Scripting via cincopa Shortcode in Post Comments in all versions up to, and including, 1.163 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation is possible because the plugin processes the [cincopa] shortcode via a comment_text filter hook, allowing unauthenticated visitors who can post comments to supply a malicious shortcode argument that persists in the database.	2026-06-24	7.2	CVE-2026-10092
nicolargo--glances	Glances is an open-source system cross-platform monitoring tool. Prior to 4.5.5, the Glances KVM/QEMU monitoring engine (glances/plugins/vms/engines/virsh.py) passes VM domain names, read directly from virsh list --all output, into f-string command templates that are processed by secure_popen(). secure_popen() is explicitly designed to interpret &&, , and > as shell operators. Because domain names are never sanitised before interpolation, any user with the ability to create or rename a KVM/QEMU virtual machine can execute arbitrary commands as the OS user running Glances - commonly root on hypervisor hosts. This vulnerability is fixed in 4.5.5.	2026-06-25	7.8	CVE-2026-46606
nicolargo--glances	Glances is an open-source system cross-platform monitoring tool. Prior to 4.5.5, glances/outdated.py uses pickle.load() to read a version-check cache file stored at a predictable, world-accessible path (~/.cache/glances/glances-version.db or \$XDG_CACHE_HOME/glances/glances-version.db). No integrity check, signature verification, or format validation is performed before deserialization. An attacker with write access to that path - through any of several realistic local or container-level scenarios - can plant a malicious pickle file and achieve arbitrary code execution as the OS user running Glances the next time it starts with version checking enabled (the default). This vulnerability is fixed in 4.5.5.	2026-06-25	7.8	CVE-2026-46607
nicolargo--glances	Glances is an open-source system cross-platform monitoring tool. Prior to 4.5.5, the Glances XML-RPC server (glances -s) introduced a configurable CORS origin list in version 4.5.3 as a mitigation for CVE-2026-33533. However, the implementation silently falls back to Access-Control-Allow-	2026-06-25	7.4	CVE-2026-46608

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Origin: * whenever cors_origins contains more than one entry. An operator who configures an explicit two-entry allowlist (e.g. two internal dashboard origins) intending to restrict browser access instead receives the unrestricted wildcard. A malicious web page served from any origin can issue a CORS simple request to /RPC2 and read the full system monitoring dataset without the victim's knowledge. This vulnerability is fixed in 4.5.5.			
nicolargo--glances	Glances is an open-source system cross-platform monitoring tool. From 4.0.8 until 4.5.5, the secure_popen() function in glances/secure.py interprets > (file redirection), (pipe), and && (command chaining) operators in command strings. These operators are applied without any validation on the target file path, piped command, or chained command. When Application Monitoring Process (AMP) modules load their command or service_cmd configuration values from glances.conf, those values are passed directly to secure_popen() with no sanitization. This allows an attacker who can modify the Glances configuration file to write arbitrary content to arbitrary filesystem paths (via >), chain arbitrary commands (via &&), or pipe command output to arbitrary programs (via). This vulnerability is fixed in 4.5.5.	2026-06-25	7.8	CVE-2026-53925
nlTK--nlTK	NLTK (Natural Language Toolkit) is a suite of open source Python modules, data sets, and tutorials supporting research and development in Natural Language Processing. Prior to 3.10.0-rc1, nltk.data.load() in NLTK is vulnerable to path traversal via URL-encoded path separators and traversal segments when using the nltk: URL scheme. The unsafe-path regex check is performed before url2pathname() decodes the %xx sequences (a classic decode-after-check / TOCTOU-style flaw), allowing an attacker to bypass the protection documented in NLTK's SECURITY.md and read arbitrary files from the filesystem. While literal traversal strings such as ../../etc/passwd are correctly blocked, encoded variants such as %2fetc%2fpasswd, %2e%2e%2f..., and ../%2f.%2f slip past the regex and are subsequently decoded into a real filesystem path. This vulnerability is fixed in 3.10.0-rc1.	2026-06-22	7.5	CVE-2026-54293
nmedia--Frontend File Manager Plugin	The Frontend File Manager Plugin plugin for WordPress is vulnerable to Authenticated Arbitrary File Deletion in versions up to and including 23.6. This is due to a case-sensitive bypass of the wpfm_dir_path parameter sanitization in the wpfm_file_meta_update AJAX handler, where supplying WPFM_DIR_PATH in uppercase evades the unset check and is normalized to wpfm_dir_path by sanitize_key() during update_post_meta(), allowing an attacker to overwrite the stored file path with an arbitrary filesystem path that is then passed directly to unlink() in delete_file_locally() without any directory containment validation. This makes it possible for authenticated attackers with Subscriber-level access to delete arbitrary files on the server, including sensitive files such as wp-config.php, potentially leading to full site takeover.	2026-06-27	8.1	CVE-2026-8095
notepad-plus-plus--notepad-plus-plus	Notepad++ is a free and open-source source code editor. Prior to 8.9.6.1, the <GUIConfig name="commandLineInterpreter"> tag in config.xml is read by NppXml::value() (Parameters.cpp:6430) and stored in _nppGUI._commandLineInterpreter without any validation, whitelist, or digital signature check. When the user triggers IDM_FILE_OPEN_CMD (File â€™ Open Containing Folder â€™ cmd), NppCommands.cpp:228 creates a Command object with this value and calls run(), which invokes ShellExecute (RunDlg.cpp:221) with the attacker-controlled string as the executable path. This vulnerability is fixed in 8.9.6.1.	2026-06-26	7.8	CVE-2026-48778
notepad-plus-plus--notepad-plus-plus	Notepad++ is a free and open-source source code editor. Prior to 8.9.6.1, the <Command> tag text content inside <UserDefinedCommands> in shortcuts.xml is read by NppXml::value(aNode) (Parameters.cpp:3658) in the feedUserCmds() function and stored in UserCommand._cmd without any validation. When the user clicks the corresponding entry in the Run menu, NppCommands.cpp:4264 creates a Command object with	2026-06-26	7.8	CVE-2026-48800

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	string2wstring(ucmd.getCmd()) and calls run(), which invokes ShellExecute (RunDlg.cpp:221) with the attacker-controlled string as the executable path. The injected command appears as a normal menu item in the Run menu, making it a viable persistence mechanism. This vulnerability is fixed in 8.9.6.1.			
notepad-plus-plus--notepad-plus-plus	Notepad++ is a free and open-source source code editor. In v8.9.6.1, isInTrustedDirectory() does NOT canonicalize the path before checking. It uses a prefix-based check (PathIsPrefix() or equivalent) that matches paths starting with trusted directory strings. A path traversal using ..\..\ after a trusted directory prefix passes the check while resolving to an untrusted location. The CVE-2026-48800 patch adds isInTrustedDirectory() validation in Command::run() (RunDlg.cpp) before calling ShellExecute(). This function checks whether the resolved executable path is under a trusted directory. This vulnerability is fixed in 8.9.6.2.	2026-06-26	7.8	CVE-2026-52884
NSquared--Simply Schedule Appointments	Unauthenticated Cross Site Scripting (XSS) in Simply Schedule Appointments <= 1.6.12.2 versions.	2026-06-26	7.1	CVE-2026-57317
Online Web Tutor--Library Management System	Unauthenticated SQL Injection in Library Management System <= 3.5.7 versions.	2026-06-26	9.3	CVE-2026-56034
oooorgle--Quotes llama	Unauthenticated SQL Injection in Quotes llama <= 3.1.5 versions.	2026-06-26	9.3	CVE-2026-56062
Open Health Imaging Foundation (OHIF)--DICOM Web Viewer Framework	Two data sources (DICOMWebProxy and DICOMJSON) shipped in the default configuration fetch an arbitrary URL parameter without validation. A global authentication service in OHIF automatically injects the authenticated user's OIDC Bearer token into the resulting requests, sending it to the attacker-controlled server. DICOMweb data sources are not impacted.	2026-06-25	8.2	CVE-2026-12473
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, backend/open_webui/utls/oauth.py::_process_picture_url calls validate_url(picture_url) on the initial URL only, then invokes aiohttp.ClientSession.get(picture_url, ...) without allow_redirects=False. aiohttp's default is allow_redirects=True, max_redirects=10; the function does not pass the project's AIOHTTP_CLIENT_ALLOW_REDIRECTS env constant either. An attacker with a valid OAuth IdP identity can therefore submit a public URL that 302-redirects to an internal address and read the internal response body via the attacker's own profile_image_url field. This vulnerability is fixed in 0.9.6.	2026-06-23	8.5	CVE-2026-54008
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, Open WebUI lets an authenticated user attach arbitrary file_id values to their own chat message without checking whether they own or can read those files. If the attacker then shares that chat and grants themselves read access, has_access_to_file() treats the victim file as accessible through the shared chat, and the file endpoints read or delete the victim file. This vulnerability is fixed in 0.9.6.	2026-06-23	8.3	CVE-2026-54010
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, Open WebUI renders Mermaid blocks from Markdown files in the file preview panel and inserts the generated SVG into the DOM using innerHTML. Because Mermaid is configured with securityLevel: 'loose', attacker-controlled Mermaid content can be rendered unsafely in this flow. A working payload was validated through the Markdown preview path, resulting in JavaScript execution in the victim's browser under the application origin. This vulnerability is fixed in 0.9.6.	2026-06-23	8.7	CVE-2026-54011
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, Open WebUI lets a user who can create, update, or import workspace models store arbitrary	2026-06-23	7.1	CVE-2026-54012

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	meta.knowledge entries on their model without checking whether they own or can read the referenced files. Open WebUI then treats meta.knowledge entries of type file as an authorization source in two places: the built-in view_file tool reads the file's extracted text, and has_access_to_file()'s model branch authorizes the file content and file delete endpoints. A malicious model owner can therefore attach another user's file ID to their model metadata and read or delete that private file. This vulnerability is fixed in 0.9.6.			
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, Open WebUI patched SVG XSS in user profile images and webhook profile images but forgot to apply the same fix to model profile images. The ModelMeta class has no validate_profile_image_url field validator, and the model image serving endpoint has no MIME allowlist or nosniff header. Any authenticated user with workspace.models permission (enabled by default) can store a data:image/svg+xml;base64,... payload in a model's profile image and achieve full account takeover of anyone who navigates to the image URL. This vulnerability is fixed in 0.9.6.	2026-06-23	7.6	CVE-2026-54013
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, the SafePlaywrightURLLoader implements a validate_url function to prevent SSRF attacks by checking the IP address of the user-provided URL. However, this validation is performed only on the initial URL. Since Playwright automatically follows HTTP redirects (301/302) by default, an attacker can bypass the validation by providing a safe URL that redirects to a restricted internal network address (e.g., localhost, Docker container network, or Cloud Metadata). This allows the application to access internal services despite ENABLE_RAG_LOCAL_WEB_FETCH being set to False This vulnerability is fixed in 0.9.6.	2026-06-23	7.7	CVE-2026-54018
OpenBSD--OpenBSD	sys/kern/sysv_sem.c in OpenBSD through 7.9 has a use-after-free allowing local privilege escalation to root. This is a context switch use-after-free after tsleep in sys_semget().	2026-06-25	7.4	CVE-2026-57589
openremote--openremote	OpenRemote before 1.25.0 contains an insecure direct object reference (IDOR) vulnerability in the bulk alarm deletion endpoint that allows authenticated users to permanently delete alarms belonging to other tenants by supplying arbitrary alarm IDs. The removeAlarms() method in AlarmResourceImpl.java omits realm-scoping validation in its JPA query, enabling any user with alarm-write permissions to enumerate sequential auto-increment alarm IDs and delete cross-tenant alarm records without authorization.	2026-06-23	8.1	CVE-2026-56784
opf--openproject	OpenProject is open-source, web-based project management software. Prior to , the official openproject/openproject Docker image ships ENV SECRET_KEY_BASE=OVERWRITE_ME as the default Rails master key. Combined with cookies_serializer = :marshal, this gives any logged-in user a deterministic Marshal-deserialization path reachable via the /my/two_factor_devices cookie reader This vulnerability is fixed in .	2026-06-26	9.9	CVE-2026-46386
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.3.3 and 17.4.1, cache store poisoning leads to Remote Code Execution (RCE). This vulnerability is fixed in 17.3.3 and 17.4.1.	2026-06-26	9.6	CVE-2026-52780
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.3.3 and 17.4.1, there is an IDOR through /projects/<A>/settings/project_storages/<A_ps_id> via PATCH parameter "storages_project_storage[project_folder_id]" leads to Access to Unauthorized Resources. A project-admin in one project can hijack the managed Nextcloud or OneDrive folder of another project on the same storage by writing the victim project's project_folder_id into the attacker's Storages::ProjectStorage row. The next managed-folder sync overwrites the ACL on the referenced folder with the attacker project's user list. This vulnerability is fixed in 17.3.3 and 17.4.1.	2026-06-26	9.9	CVE-2026-52782

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.3.3 and 17.4.1, there is a SQL injection in timestamps functionality. OpenProject baseline comparison allows callers to request historic work-package attributes using the timestamps parameter. This vulnerability is fixed in 17.3.3 and 17.4.1.	2026-06-26	9.9	CVE-2026-52785
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.3.3 and 17.4.1, OpenProject's Storages module writes the OneDrive/SharePoint userless OAuth access_token plaintext to Rails.cache under the deterministic key storage.<id>.httpx_access_token, repopulated continuously by an hourly cron and every userless-OAuth call site (see Write cadence). None of the three allowed cache backends (file_store, memcache, redis) encrypts at rest. An attacker with read access to the cache backend recovers the Azure-AD application-tier bearer with an anonymous get over the memcached binary protocol (or the equivalent against Redis). This vulnerability is fixed in 17.3.3 and 17.4.1.	2026-06-26	8.2	CVE-2026-52783
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.3.3 and 17.4.1, there is a CSRF on TARGET through /users/:id via POST parameter "user[admin]". This vulnerability is fixed in 17.3.3 and 17.4.1.	2026-06-26	8.8	CVE-2026-52784
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.3.3 and 17.4.1, the journal diff endpoint discloses hidden historical field values without enforcing object and field visibility. This vulnerability is fixed in 17.3.3 and 17.4.1.	2026-06-26	7.5	CVE-2026-47193
pagekit--pagekit	Pagekit CMS 1.0.18 contains a privilege escalation vulnerability that allows authenticated users with the 'user: manage users' permission to escalate privileges by assigning arbitrary custom roles to themselves due to missing authorization checks in UserApiController::saveAction(). Attackers can assign themselves a custom role with the 'system: manage packages' permission and then upload and install a malicious PHP package through the admin package installer to achieve remote code execution.	2026-06-26	8.8	CVE-2026-57518
Paolo--GeoDirectory	Unauthenticated SQL Injection in GeoDirectory <= 2.8.162 versions.	2026-06-26	9.3	CVE-2026-54831
parse-community--parse-server	Parse Server before 4.10.0 contains a supply chain vulnerability where incorrect version tags were pushed to the repository linking to unreviewed code in a personal fork. Attackers could exploit this by specifying affected version tags in dependency declarations to execute unreviewed and potentially malicious code.	2026-06-25	7.5	CVE-2021-47986
parse-community--parse-server	Parse Server before 4.10.0 was affected by a supply chain incident in which incorrect version tags were pushed to the official repository pointing to an unreviewed personal fork of a contributor with write access. No releases were published with these tags; a project was exposed only if it defined a git-based dependency referencing one of the affected tags (for example, parse-server#4.9.3). The code behind the tags was not reviewed or approved, and although no malicious code was identified, the introduction of security vulnerabilities could not be ruled out.	2026-06-25	7.5	CVE-2021-47987
Paymob--Paymob for WooCommerce	Unauthenticated Broken Access Control in Paymob for WooCommerce <= 4.1.2 versions.	2026-06-26	7.5	CVE-2026-56025
paytiumsupport--Paytium	Unauthenticated Privilege Escalation in Paytium <= 5.0.2 versions.	2026-06-26	9.8	CVE-2026-56030
Peplink--InControl	Peplink InControl 2 through 2.14.2 before 2026-06-03 allows use of a semicolon to bypass access-control rules for certain /rest/o/{orgId} endpoints.	2026-06-26	7.7	CVE-2026-57920
Perfmatters, Powered Kinsta + GeneratePress Docs Changelog Feature requests Legal Affiliate	Unauthenticated Cross Site Scripting (XSS) in perfmatters <= 2.6.3 versions.	2026-06-26	7.1	CVE-2026-56047

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Contact--perfmatters				
PhysCode--Travel Booking	Subscriber Arbitrary File Upload in Travel Booking <= 2.2.5 versions.	2026-06-26	9.9	CVE-2026-56059
Picklescan--Picklescan	Picklescan before 0.0.33 fails to detect the numpy.f2py.crackfortran._eval_length gadget in pickle __reduce__ methods, allowing arbitrary code execution. Attackers can craft malicious pickle files that execute arbitrary Python code when loaded by victims who trust Picklescan's safety validation.	2026-06-22	8.1	CVE-2025-71339
picklescan--picklescan	picklescan before 1.0.4 fails to block at least seven Python standard library modules (including uuid, _osx_support, _aix_support, _pyrepl.pager, and imaplib) exposing eight functions that provide direct arbitrary command execution. Attackers can craft malicious pickle files importing these unblocked modules to achieve remote code execution while bypassing picklescan's safety validation entirely.	2026-06-23	9.8	CVE-2026-56315
picklescan--picklescan	picklescan through 0.0.26 fails to detect malicious pickle files that invoke idlib.pyshell.ModifiedInterpreter.runcode in __reduce__ methods. Attackers can embed undetected code in pickle files that executes arbitrary commands when the file is loaded via pickle.load(), enabling supply chain attacks on PyTorch models and saved Python objects. This is fixed in version 0.0.30.	2026-06-25	8.1	CVE-2025-71340
picklescan--picklescan	picklescan before 0.0.29 fails to detect the profile.Profile.runtx function when analyzing pickle files, allowing attackers to embed undetected malicious code. Remote attackers can craft malicious pickle files using profile.Profile.runtx in the reduce method to achieve remote code execution when the pickle file is loaded.	2026-06-23	8.1	CVE-2025-71341
picklescan--picklescan	picklescan before 0.0.30 (affected versions 0.0.26 and earlier) fails to detect the ensurepip._run_pip built-in function when scanning pickle files, allowing attackers to execute arbitrary code. Malicious pickle files embedding ensurepip._run_pip calls in __reduce__ methods bypass picklescan detection and achieve remote code execution upon pickle.load() invocation.	2026-06-22	8.1	CVE-2025-71344
picklescan--picklescan	picklescan before 0.0.29 fails to detect malicious pickle files that exploit idlib.debugobj.ObjectTreeItem.SetText function in reduce methods. Attackers can craft pickle files with embedded code that bypasses picklescan detection and executes arbitrary commands when pickle.load() is called.	2026-06-24	8.1	CVE-2025-71354
picklescan--picklescan	picklescan before 0.0.29 fails to detect malicious pickle files that exploit idlib.autocomplete.AutoComplete.get_entity function in reduce methods. Attackers can embed undetected code in pickle files that executes arbitrary commands when loaded by victims using pickle.load().	2026-06-22	8.1	CVE-2025-71358
picklescan--picklescan	picklescan before 0.0.29 fails to detect malicious idlib.calltip.Calltip.fetch_tip calls in pickle files, allowing remote code execution. Attackers can embed undetected payloads in pickle files that execute arbitrary code when loaded via pickle.load().	2026-06-24	8.1	CVE-2025-71361
picklescan--picklescan	picklescan before 0.0.33 fails to detect malicious pickle files that invoke numpy.f2py.crackfortran.myeval function through the reduce method. Attackers can craft malicious pickle files embedding arbitrary code that evades picklescan detection and executes remote code when loaded.	2026-06-23	8.1	CVE-2025-71365
picklescan--picklescan	picklescan before 0.0.28 fails to detect malicious torch.jit.unsupported_tensor_ops.execWrapper function calls embedded in pickle files. Attackers can craft malicious pickle files that bypass picklescan detection and execute arbitrary code when loaded via pickle.load().	2026-06-23	8.1	CVE-2025-71370
picklescan--picklescan	picklescan before 0.0.29 fails to detect malicious pickle files using idlib.autocomplete.AutoComplete.fetch_completions in reduce methods. Attackers can embed undetected code in pickle files that executes arbitrary commands when loaded by victims.	2026-06-23	8.1	CVE-2025-71376

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Pilz--PMI v8xx	A stored cross-site scripting vulnerability in the Runtime component of Pilz PASvisu before 1.14.1 and PMI v8xx up to and including 2.0.33992 allows a low-privileged remote unauthenticated attacker to manipulate process data with potential impact on integrity and/or availability.	2026-06-22	8.1	CVE-2023-45796
Pilz--PMI v8xx	A cross-site scripting vulnerability in the Builder Component of Pilz PASvisu before 1.14.1 allows a local unauthenticated attacker to inject malicious javascript and gain full control over the device.	2026-06-22	7.8	CVE-2023-45795
piscinajs--piscina	piscina is a node.js worker pool implementation. Prior to 6.0.0-rc.2, 5.2.0, and 4.9.3, piscina's constructor and run() paths read the filename option via plain member access. Both reads fall through the prototype chain when the caller's options object doesn't have filename as an own property. When Object.prototype.filename is polluted upstream the inherited value flows to worker_threads.Worker import and the attacker's .mjs runs in the worker. This vulnerability is fixed in 6.0.0-rc.2, 5.2.0, and 4.9.3.	2026-06-22	8.1	CVE-2026-55388
Pluggabl--Booster for WooCommerce	Customer Arbitrary File Upload in Booster for WooCommerce <= 8.0.1 versions.	2026-06-26	9.9	CVE-2026-56027
PluginUs.Net--MDTF	Unauthenticated SQL Injection in MDTF <= 1.3.7 versions.	2026-06-25	9.3	CVE-2026-54843
PluginUs.Net--MDTF	Unauthenticated Local File Inclusion in MDTF <= 1.3.8 versions.	2026-06-25	8.1	CVE-2026-54845
pnpm--pnpm	pnpm is a package manager. Prior to 10.34.0 and 11.4.0, pnpm allows a transitive dependency alias from registry package metadata to contain path traversal segments. During install, pnpm later uses that alias as a filesystem path when linking dependency nodes. As a result, a registry package can cause `pnpm install --ignore-scripts` to replace paths in the current project with symlinks to attacker-controlled dependency package directories. This vulnerability is fixed in 10.34.0 and 11.4.0.	2026-06-25	8.8	CVE-2026-50016
pnpm--pnpm	pnpm is a package manager. Prior to 10.34.2 and 11.5.3, pnpm can persist package-manager bootstrap metadata in the first YAML document of pnpm-lock.yaml. Before the patch, direct pnpm execution trusted an already resolved packageManagerDependencies entry when the committed env lockfile contained matching pnpm and @pnpm/exe versions. A malicious repository could therefore commit package-manager lockfile package records and snapshots that bypassed fresh package-manager resolution, then cause pnpm to install and execute bytes selected by that committed lockfile state during automatic version switching. This vulnerability is fixed in 10.34.2 and 11.5.3.	2026-06-25	8.8	CVE-2026-55698
pnpm--pnpm	pnpm is a package manager. Prior to 10.34.0 and 11.4.0, pnpm's patch application pipeline (@pnpm/patch-package) performs no path validation on file paths extracted from .patch files. An attacker who contributes a malicious patch file via a pull request can write attacker-controlled content to or delete arbitrary files on the filesystem during pnpm install, as the user running the install. The diff --git header paths containing ../../ sequences traverse out of the package directory, and the traversal is difficult to catch in code review because patch file diff headers are opaque to most reviewers. This vulnerability is fixed in 10.34.0 and 11.4.0.	2026-06-25	7.3	CVE-2026-50015
pnpm--pnpm	pnpm is a package manager. Prior to 10.34.2 and 11.5.3, the generic peer-suffix normalizer also stripped parenthesized text from git, URL, tarball, file, and other opaque locators. Approval for one source string could therefore authorize a different attacker-controlled source whose locator normalized to the same value. This vulnerability is fixed in 10.34.2 and 11.5.3.	2026-06-25	7.5	CVE-2026-55487
pnpm--pnpm	pnpm is a package manager. Prior to 10.34.2 and 11.5.3, pnpm can install configDependencies declared in pnpm-workspace.yaml before command dispatch. Before the patch, a repository could declare pacquet or @pnpm/pacquet as a config dependency and pnpm treated that repository-controlled dependency as an install-engine opt-in. During install, pnpm resolved a platform-specific @pacquet/<platform>-	2026-06-25	7.5	CVE-2026-55697

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	<arch>/pacquet binary from node_modules/.pnpm-config/<packageName> and spawned it as the developer or CI user. This vulnerability is fixed in 10.34.2 and 11.5.3.			
pnpm--pnpm	pnpm is a package manager. From 11.3.0 until 11.5.3, `pnpm stage download` derived a local filename from registry-controlled package name and version fields. A crafted manifest could escape the selected download directory and overwrite another reachable file. The merged fix validates both fields, derives one safe filename, and verifies the final destination before writing. This vulnerability is fixed in 11.5.3.	2026-06-25	7.1	CVE-2026-55700
podman-container-tools--podman	Podman is a tool for managing OCI containers and pods. From 1.8.1 until 5.8.4, a container image that contains a environment variable with just a key and no value can trick podman into passing that variable from the host into the container. This is made worse by the fact that using an asterisk (*) will cause podman to pass all host variables into the container. So essentially a malicious image can exfiltrate all podman environment variables that are set in the session from where the container is launched. This vulnerability is fixed in 5.8.4 and 6.0.0.	2026-06-26	7.5	CVE-2026-57231
Post Snippets--Post Snippets	Contributor Remote Code Execution (RCE) in Post Snippets <= 4.0.19 versions.	2026-06-25	8.5	CVE-2026-56049
poweradmin--poweradmin	Poweradmin is a web-based DNS administration tool for PowerDNS server. Versions prior to 4.2.4 and 4.3.3 use the attacker-controlled `HTTP_HOST` request header as the authoritative source for building callback URLs in its OIDC, SAML, and logout authentication flows without any validation. An unauthenticated attacker can poison the `redirect_uri` sent to the Identity Provider, causing the IdP to redirect the victim's authorization code to an attacker-controlled server - resulting in full account takeover with no credentials required. Versions 4.2.4 and 4.3.3 patch the issue.	2026-06-23	9.6	CVE-2026-54588
PowerDNS--Recursor	A malicious authoritative server can send a crafted zone via the ZoneToCache function that leads to cache poisoning.	2026-06-25	7.5	CVE-2026-33612
pravel--Invoice Generator	The Invoice Generator plugin for WordPress is vulnerable to privilege escalation due to a missing capability check on the pravel_invoice_edit_account() AJAX action in versions up to, and including, 1.0.0. The handler is exposed via wp_ajax_nopriv_pravel_invoice_edit_account, accepts an attacker-controlled user_id and user_email from POST data, and calls wp_update_user() without verifying authentication, ownership, or a nonce. This makes it possible for unauthenticated attackers to change the email address of any user, including administrators, and then trigger WordPress's password reset flow to gain access to the targeted account.	2026-06-27	9.8	CVE-2026-12415
pravel--Invoice Generator	The Invoice Generator plugin for WordPress is vulnerable to Account Takeover via Password Reset in all versions up to, and including, 1.0.0. This is due to the `pravel_invoice_change_password()` function being registered as a nopriv AJAX handler with no nonce verification and no authorization check, and performing a loose equality comparison between the supplied `reset_activation_code` POST parameter and the target user's stored `forgot_email` user meta - a check that trivially evaluates to true ("" == "") for any user who has never initiated a forgot-password request, which applies to administrators under normal conditions. This makes it possible for unauthenticated attackers to supply an arbitrary user ID via the `reset_user_id` POST parameter, bypass the activation code check entirely by omitting `reset_activation_code`, and set the target account's password to an attacker-chosen value, enabling full takeover of any account on the site, including administrator accounts.	2026-06-24	9.8	CVE-2026-12416
pravel--SignUp & SignIn	The SignUp & SignIn plugin for WordPress is vulnerable to Authentication Bypass via Weak Password Reset Validation leading to Account Takeover in versions up to, and including, 1.0.0. This is due to the `pravel_change_password()` AJAX handler - registered via `wp_ajax_nopriv_pravel_change_password` and therefore accessible to unauthenticated users - performing no nonce verification, no capability	2026-06-24	9.8	CVE-2026-12417

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	check, and only a loose equality check between an attacker-supplied `reset_activation_code` POST parameter and the target user's `forgot_email` user meta value; when a user has never initiated a password reset, `get_user_meta()` returns an empty string that trivially satisfies this check against an omitted or empty attacker-supplied code. This makes it possible for unauthenticated attackers to change the password of any WordPress user, including administrators, by sending a crafted POST request to `admin-ajax.php` with `action=pravel_change_password`, `reset_user_id` set to the target account's user ID, and `new_password_custom` set to an attacker-chosen password. Successful exploitation allows the attacker to authenticate with the newly set password and fully take over the targeted account, achieving administrator-level privilege escalation on the affected site.			
Premmerce-- Premmerce Wishlist for WooCommerce	Unauthenticated SQL Injection in Premmerce Wishlist for WooCommerce <= 1.1.11 versions.	2026-06-25	9.3	CVE-2026-54849
presire-- qSnapper	A time-to-check-time-of-use in polkit authentication of qSnapper before version 1.3.3 allowed a local attacker to bypass qSnappers authentication mechanism and operate e.g. as root user.	2026-06-22	8.1	CVE-2026-41045
presire-- qSnapper	A path traversal attack when using a "configName" parameter in qSnapper before version 1.3.3 allowed a local attacker to use malicious config files for snapper and so cause a denial of service or potentially escalate privileges to root.	2026-06-22	7.3	CVE-2026-41046
ProFTPD Project-- ProFTPD	ProFTPD through 1.3.9b and 1.3.10rc2 contains an access control bypass vulnerability that allows authenticated FTP users to circumvent Directory ACL restrictions by prefixing paths with /proc/self/root in the RNFR command handler. Attackers can exploit the unresolved symlink components in dir_canonical_path() to cause dir_check() to perform lexical path comparisons that match no configured Directory block, enabling rename operations on files in DenyAll-protected directories and subsequent retrieval of those files. Mitigation: Sessions configured with DefaultRoot (chroot) are not affected, as chroot changes the directory to which /proc/self/root resolves.	2026-06-24	8.1	CVE-2026-35025
protobufjs-- protobuf.js	protobufjs compiles protobuf definitions into JavaScript (JS) functions. Prior to 7.6.1 and 8.4.1, protobufjs could recurse without a depth limit while converting decoded messages to plain objects or JSON. This affected generated toObject() conversion and the custom google.protobuf.Any JSON conversion path. A crafted protobuf binary payload containing deeply nested Any values could cause the JavaScript call stack to be exhausted during conversion to JSON. This vulnerability is fixed in 7.6.1 and 8.4.1.	2026-06-22	7.5	CVE-2026-48712
protobufjs-- protobufjs-cli	protobufjs-cli is the command line add-on for protobuf.js. Prior to 1.3.2 and 2.5.0, a previous fix for unsafe name handling in pbjs static / static-module code generation was incomplete. Affected versions of protobufjs-cli could still emit unsafe JavaScript references when generating static output from crafted JSON descriptor input. The common case of parsing schemas from .proto files is not affected. This is a bypass of CVE-2026-44295. An attacker who can provide or influence pre-parsed JSON descriptors passed to pbjs static code generation may be able to cause generated JavaScript output to contain attacker-controlled code. The injected code may execute if the generated file is later executed or imported and an affected generated API path is invoked. This vulnerability is fixed in 1.3.2 and 2.5.0.	2026-06-22	8.2	CVE-2026-54271
PSM Plugins-- SupportCandy	Subscriber Insecure Direct Object References (IDOR) in SupportCandy <= 3.4.6 versions.	2026-06-26	7.6	CVE-2026-54826
pydicom-- pynetdicom Library	The qrscp application's C-STORE handler uses a specific instance from attacker-supplied DICOM datasets directly in os.path.join() without sanitization, allowing file writes to arbitrary paths.	2026-06-25	9.1	CVE-2026-56445

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Rapid7--InsightConnect AWK Plugin	OS Command Injection vulnerability in the process_string action of Rapid7 InsightConnect AWK Plugin on Linux allows remote attackers to execute arbitrary OS commands via the text or expression parameters due to unsafe shell command construction in the processing pipeline.	2026-06-25	7.7	CVE-2026-8592
Rapid7--InsightConnect Ping Plugin	OS Command Injection vulnerability in the ping action of Rapid7 InsightConnect Ping Plugin on Linux allows remote attackers to execute arbitrary OS commands via the host parameter due to insufficient input validation when constructing shell commands.	2026-06-25	7.7	CVE-2026-8660
Rapid7--InsightConnect Sed Plugin	OS Command Injection vulnerability in Rapid7 InsightConnect Sed Plugin on Linux allows authenticated attackers to execute arbitrary OS commands via the expression parameter due to insufficient input validation.	2026-06-25	8.8	CVE-2026-9155
Rapid7--InsightConnect Sed Plugin	Arbitrary File Write vulnerability in Rapid7 InsightConnect Sed Plugin on Linux allows authenticated attackers to write attacker-controlled content to arbitrary file paths via the expression parameter.	2026-06-25	7.1	CVE-2026-9154
Rapid7--InsightConnect TR Plugin	OS Command Injection vulnerability in the TR action of Rapid7 InsightConnect Translate Plugin on Linux allows remote attackers to execute arbitrary OS commands via the text or expression parameters due to insufficient input sanitization in shell command construction.	2026-06-25	7.7	CVE-2026-8665
Rapid7--InsightConnect Traceroute Plugin	OS Command Injection vulnerability in the traceroute action of Rapid7 InsightConnect Traceroute Plugin on Linux allows remote attackers to execute arbitrary OS commands via the host, port, max_ttl, count, or time_out request parameters due to insufficient input validation when constructing shell commands.	2026-06-25	7.7	CVE-2026-8666
rasta-mouse--pwnlift	pwnlift before d7a9544, in a privileged deployment, contains a symlink following vulnerability in the upload handler in Components/Pages/Home.razor.	2026-06-23	7.4	CVE-2026-56815
rclone--rclone	Rclone is a command-line program to sync files and directories to and from different cloud storage providers. From 1.46.0 until 1.74.3, rclone rcd --rc-serve accepts unauthenticated GET and HEAD requests to paths of the form: /[remote:path]/object. The remote value is parsed from the URL and passed to normal backend initialization. Inline remote configuration can set backend options that execute local commands during initialization. As a result, a single unauthenticated GET or HEAD request can execute a command as the rclone process user. This vulnerability is fixed in 1.74.3.	2026-06-24	9.8	CVE-2026-49980
RealMag777--FOX	Unauthenticated Cross Site Scripting (XSS) in FOX <= 1.4.8 versions.	2026-06-26	7.1	CVE-2026-57319
Red Hat--Red Hat Ansible Automation Platform 2.5 for RHEL 8	A missing authorization vulnerability was found in the Event-Driven Ansible (EDA) websocket API. The /api/eda/ws/ansible-rulebook endpoint does not verify user permissions when processing Worker messages. Any authenticated user can send a forged message with an arbitrary activation_id to receive plaintext credentials associated with that activation, including OAuth tokens, vault passwords, and SSH keys.	2026-06-23	9.6	CVE-2026-11807
Red Hat--Red Hat build of Apicurio Registry 3	A flaw was found in Apicurio Registry. The ContentTypeUtil.isParsableXml() method creates a SAXParserFactory without enabling secure processing features or disabling external entity resolution. An attacker with artifact-write permission (or unauthenticated when the registry runs with default configuration) can upload a crafted XML document to trigger blind server-side request forgery (SSRF) via external DTD/entity fetch, or cause denial of service via entity expansion.	2026-06-25	8.5	CVE-2026-12975
Red Hat--Red Hat build of Apicurio Registry 3	A flaw was found in Apicurio Registry. The WSDLReaderAccessor creates a wsdl4j WSDLReader without disabling the javax.wsdl.importDocuments feature. When the VALIDITY rule is set to FULL, an attacker with Developer-role access can upload a WSDL document containing attacker-controlled import locations, causing the registry to issue HTTP requests to arbitrary internal URLs (server-side request forgery).	2026-06-25	7.4	CVE-2026-12992
Red Hat--Red Hat build of Keycloak 26.4	A flaw was found in Keycloak Policy Enforcer. This vulnerability allows any authenticated user to bypass all authorization policies, including role, scope, and User-Managed Access (UMA) permission checks. By including the configured access-denied page path within a request URL, either as a	2026-06-25	8.1	CVE-2026-9800

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	path segment or a query parameter, an attacker can gain unauthorized access to protected resources.			
Red Hat--Red Hat build of Keycloak 26.4	A flaw was found in Keycloak. A remote attacker with administrative privileges, specifically those with `manage-client` permission or access to client registration endpoints, could bypass client Uniform Resource Identifier (URI) validation. This is achieved by registering a malicious client with a specially crafted redirect URI using a case-insensitive `javascript:` or `data:` scheme. This Cross-Site Scripting (XSS) vulnerability allows for arbitrary code execution in the Keycloak origin when a victim clicks the crafted link, such as in the logout flow or the Admin Console.	2026-06-25	7.3	CVE-2026-9086
Red Hat--Red Hat build of Keycloak 26.4	A flaw was found in Keycloak. A missing authorization check in the GroupResource.addChild() endpoint within the Admin REST API allows an authenticated user with limited administrative privileges to reparent any existing group. When Fine-Grained Admin Permissions v2 (FGAPv2) is enabled, an attacker with management rights over a single low-privilege group can reparent a highly privileged group (such as one possessing the realm-admin role) under their managed group. Because group permissions follow a hierarchical structure, this action unauthorizedly grants the attacker management and password-reset capabilities over the members of the targeted privileged group. An attacker can exploit this to reset an administrator's password, compromise the account, and achieve a full realm takeover, leading to a complete compromise of confidentiality, integrity, and availability.	2026-06-25	7.7	CVE-2026-9099
Red Hat--Red Hat build of Keycloak 26.6	A flaw was found in Keycloak. This JWT algorithm confusion vulnerability in the JWT Authorization Grant flow allows an attacker with valid client credentials to bypass signature verification. By forging an assertion, the attacker can create unauthorized access tokens. This enables the attacker to impersonate any federated user linked to the affected Identity Provider, leading to unauthorized access and potential privilege escalation.	2026-06-25	8.1	CVE-2026-11800
Red Hat--Red Hat OpenShift Container Platform 4	A flaw was found in the Windows Machine Config Operator (WMCO) for Red Hat OpenShift Container Platform. The WICD CSR auto-approver validates that a Certificate Signing Request contains the organization system:wicd-nodes but does not reject additional organization values such as system:masters. A compromised Windows worker node that holds WICD credentials can submit a CSR that is auto-approved and signed by the cluster, yielding a client certificate that grants cluster-administrator privileges and enabling full cluster takeover.	2026-06-22	8.8	CVE-2026-54099
Red Hat--Red Hat OpenShift Container Platform 4	A flaw was found in the Windows Machine Config Operator (WMCO) for Red Hat OpenShift Container Platform. WMCO establishes SSH connections to Windows worker nodes without verifying the remote server host key. An adjacent-network attacker who can intercept or redirect WMCO's SSH session can capture WICD and kubelet bootstrap credentials transferred during node configuration, enabling compromise of Windows node identities in the cluster.	2026-06-22	8.3	CVE-2026-54100
Red Hat--Red Hat OpenShift Virtualization 4	A flaw was found in KubeVirt's migration proxy. When spec.configuration.migrations.disableTLS is set to true on the KubeVirt custom resource, the target virt-handler binds a plain TCP listener on all interfaces (0.0.0.0/::) on a random port with no authentication, peer allow-list, or handshake token. This listener proxies directly into the target virt-launcher's virtqemud control socket. An attacker with a running pod on the cluster network can connect to this listener and issue unfiltered libvirt RPC commands against another tenant's virtual machine, including reading VM memory and configuration, modifying VM state via QMP, or destroying the VM. The bind address is unconditionally 0.0.0.0 - configuring a dedicated migration network via migrations.network only changes the advertised migration IP, not the listener bind address, so the port remains reachable on the pod network even when a dedicated migration network is configured. The API documentation describes disableTLS as removing	2026-06-26	8.5	CVE-2026-13325

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	"the additional layer of live migration encryption" without disclosing that it also removes all mutual authentication.			
Red Hat--Red Hat OpenShift Virtualization 4	A flaw was found in KubeVirt's safepath package used by virt-handler. The OpenAtNoFollow function uses O_PATH O_NOFOLLOW to obtain a file descriptor to a path leaf, but downstream operations resolve the path via /proc/self/fd/N using link-following syscalls. When the leaf is a symlink, the kernel dereferences it, defeating the intended no-follow protection. An attacker with access to a virt-launcher pod can exploit this to redirect virt-handler's IPC socket connections, including the notify socket used for VM domain lifecycle events. By hijacking this socket, the attacker can inject arbitrary domain events into virt-handler, causing it to take incorrect lifecycle actions, corrupt VM state in the Kubernetes API, or crash - resulting in sustained denial of VM management services for all virtual machines on the affected node. Additionally, the same symlink following flaw allows virt-handler to apply file ownership or permission changes to unintended host paths.	2026-06-24	7.3	CVE-2026-13201
Red Hat--Red Hat Satellite 6.19	A flaw was found in the foreman-mcp-server. A session management vulnerability in the MCP Server allows unauthenticated attackers to hijack active administrative sessions due to an improper cache of authenticated client connections, by trusting a non-secret session ID without re-validating authentication tokens and by logging all newly created session IDs to standard logs. This issue can result in privilege escalation and infrastructure-wide code execution.	2026-06-23	7.8	CVE-2026-12112
rickknowles--Winstone Servlet Container	Winstone Servlet Engine through 0.9.10 contains a path traversal vulnerability that allows unauthenticated attackers to read arbitrary files by sending HTTP GET requests with dot-dot-slash sequences that are not sanitized when serving static files from the configured webroot. Attackers can traverse outside the webroot directory using traversal-prefixed paths in a single HTTP request to read any file accessible to the servlet engine process, including sensitive system files when the service runs with elevated privileges.	2026-06-25	7.5	CVE-2026-56122
RocketChat--Rocket.Chat	Rocket.Chat is an open-source, secure, fully customizable communications platform. Prior to 8.5.0, 8.4.1, 8.3.3, 8.2.3, 8.1.4, 8.0.5, 7.13.7, and 7.10.11, Rocket.Chat's CAS login handler forwards the client-supplied options.cas.credentialToken value straight into a MongoDB findOne({_id: ...}) query without any runtime type check. TypeScript's string parameter annotation is erased at runtime, so an unauthenticated attacker can substitute a MongoDB query operator ({ "\$gt": "" }, { "\$ne": null }, etc.) for what the server expects to be an opaque ticket string. The injected operator matches the first unexpired document in the credential_tokens collection, bypassing the CAS ticket check entirely. When any legitimate CAS or SAML SSO login is in flight, the attacker's next DDP login call matches the same credential-token row via the NoSQL operator and is issued a full Meteor auth token (userId + token) bound to the victim. The token is immediately usable against the complete REST and DDP surface as that user. If the victim is an administrator, this escalates to full instance compromise via Apps-Engine app install. This vulnerability is fixed in 8.5.0, 8.4.1, 8.3.3, 8.2.3, 8.1.4, 8.0.5, 7.13.7, and 7.10.11.	2026-06-24	9.1	CVE-2026-45688
RocketChat--Rocket.Chat	Rocket.Chat is an open-source, secure, fully customizable communications platform. Prior to 8.5.0, 8.4.1, 8.3.3, 8.2.3, 8.1.4, 8.0.5, 7.13.7, and 7.10.11, an unauthenticated network attacker obtains a valid Rocket.Chat OAuth access token for an arbitrary user by sending a single HTTP POST with MongoDB query operators to /oauth/token. The Rocket.Chat OAuth2 server does not validate that grant parameters are strings before forwarding them to findOne({...}) against the oauth_apps and oauth_access_tokens collections, so an attacker substitutes {"\$ne": null} for client_id, client_secret, and refresh_token and receives a freshly minted {access_token, refresh_token} pair bound to whichever user's refresh token Mongo returned first. The resulting access token is a first-	2026-06-24	9.1	CVE-2026-45689

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	class bearer credential against the full /api/v1/* surface as that user. By iterating with \$nin / \$regex operators the attacker walks the entire oauth_access_tokens collection, collecting one fresh access token per user per request. If any matched token belongs to an admin, the stolen bearer gives full admin API access (including Apps-Engine app installation, i.e. server-side code execution). No account, credentials, userId, or prior interaction with the instance are required. This vulnerability is fixed in 8.5.0, 8.4.1, 8.3.3, 8.2.3, 8.1.4, 8.0.5, 7.13.7, and 7.10.11.			
RocketChat-- Rocket.Chat	Rocket.Chat is an open-source, secure, fully customizable communications platform. Prior to 8.5.0, 8.4.1, 8.3.3, 8.2.3, 8.1.4, 8.0.5, 7.13.7, and 7.10.11, Rocket.Chat's sendFileMessage DDP method passes the entire attacker-supplied file object into Uploads.updateFileComplete, which merges it directly into a MongoDB \$set update via Object.assign. There is no allow-list of writable fields. An attacker can therefore rewrite any column on their own upload record, notably store and the store-specific path fields. This vulnerability is fixed in 8.5.0, 8.4.1, 8.3.3, 8.2.3, 8.1.4, 8.0.5, 7.13.7, and 7.10.11.	2026-06-24	8.5	CVE-2026-45687
RocketChat-- Rocket.Chat	Rocket.Chat is an open-source, secure, fully customizable communications platform. Prior to 8.5.1, 8.4.4, 8.3.6, 8.2.6, 8.1.6, 8.0.7, and 7.10.13, the POST /api/v1/fingerprint REST endpoint enforces authentication (authRequired: true) but performs no authorization check. Any authenticated user - including a standard user role account - can call this endpoint with {"setDeploymentAs": "new-workspace"} to permanently deregister the workspace from Rocket.Chat Cloud. This wipes all cloud credentials, removes the workspace license, breaks push notifications for all users, and requires manual re-registration to recover. This vulnerability is fixed in 8.5.1, 8.4.4, 8.3.6, 8.2.6, 8.1.6, 8.0.7, and 7.10.13.	2026-06-24	8.1	CVE-2026-55762
RocketChat-- Rocket.Chat	Rocket.Chat is an open-source, secure, fully customizable communications platform. Prior to 8.5.1, 8.4.4, 8.3.6, 8.2.6, 8.1.6, 8.0.7, and 7.10.13, Rocket.Chat's Apple Sign-In handler verifies JWT signatures but skips claims validation. Any Apple-signed JWT with a non-empty iss is accepted regardless of aud, exp, nbf, or nonce. An attacker who obtains a target user's Apple identity token (from server logs, an intercepted sign-in flow, or another application sharing the same Apple developer team) can replay it to authenticate as that user, with no expiration on the replay window. This vulnerability is fixed in 8.5.1, 8.4.4, 8.3.6, 8.2.6, 8.1.6, 8.0.7, and 7.10.13.	2026-06-24	7.4	CVE-2026-55759
Royal Plugins-- Royal MCP	Missing Authorization vulnerability in Royal Plugins Royal MCP allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Royal MCP: from n/a through 1.4.25.	2026-06-25	8.1	CVE-2026-54842
rtk-ai--rtk	rtk filters and compresses command outputs before they reach your LLM context. Prior to 0.42.2, the permission splitter did not conservatively split or reject several shell constructs that Bash treats as command execution boundaries or nested execution. As a result, a command beginning with an allowed prefix such as git could hide a second command behind one of these constructs. rtk rewrite returned exit code 0, causing the Claude hook to emit permissionDecision: "allow". The rewritten command still contained the hidden command, so it ran without the user confirmation or denial that the permission rules were intended to enforce. This vulnerability is fixed in 0.42.2.	2026-06-23	7.8	CVE-2026-54555
Rustaurius--Five Star Restaurant Menu	Unauthenticated Broken Access Control in Five Star Restaurant Menu <= 2.5.2 versions.	2026-06-26	7.5	CVE-2026-54835
RustDesk-- RustDesk	RustDesk gates incoming control messages on per-capability flags rather than on the session's authorized connection type, and a file-transfer session does not clear those flags. A peer holding only a valid FileTransfer authorization can inject keyboard and mouse input and reach the unguarded screenshot and display-capture handlers, acting outside its granted scope.	2026-06-28	7.6	CVE-2026-58056

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rustfs--rustfs	RustFS is a distributed object storage system built in Rust. In 1.0.0-beta.4, authenticated users with only PutObject permission on their own bucket can exploit a path traversal vulnerability in the Snowball auto-extract feature to write arbitrary objects into other users' buckets, completely breaking multi-tenant isolation. The vulnerability chains three flaws: No ../ sanitization in tar entry key normalization; IAM wildcard matching uses raw (uncleaned) paths; and Filesystem path cleaning resolves ../ across bucket boundaries.	2026-06-26	8.6	CVE-2026-49991
rustfs--rustfs	RustFS is a distributed object storage system built in Rust. From 1.0.0-alpha.1 until 1.0.0-beta.9, RustFS contains an authorization bypass in the bucket replication admin API. The ListRemoteTargetHandler handler for listing remote replication targets only checks whether request credentials exist, but does not verify that the caller has replication or administrator permissions. As a result, an authenticated user with no effective bucket or admin permissions can list remote replication target configuration for a bucket. Because the returned BucketTarget objects include remote target credentials, this can disclose replication access keys and secret keys. This vulnerability is fixed in 1.0.0-beta.9.	2026-06-26	8.2	CVE-2026-55188
rustfs--rustfs	RustFS is a distributed object storage system built in Rust. From 1.0.0-alpha.1 until 1.0.0-beta.9, when the FTP frontend is enabled, the FTP read and probe handlers dispatch directly to the storage backend without ever calling the IAM authorization function that the FTP write/list handlers (and the entire HTTP S3 path) use. As a result, any user who can authenticate to the FTP listener - including a user whose IAM policy contains an explicit Deny on s3:GetObject - can read (RETR) and stat (SIZE/MDTM) any object in any bucket, and probe any bucket (CWD), completely regardless of their IAM policy. This vulnerability is fixed in 1.0.0-beta.9.	2026-06-26	7.7	CVE-2026-55189
Rymera Web Co--WC Vendors Marketplace	Subscriber SQL Injection in WC Vendors Marketplace <= 2.6.8 versions.	2026-06-25	8.5	CVE-2026-54838
Saad Iqbal--APIExperts Square for WooCommerce	Insertion of Sensitive Information Into Sent Data vulnerability in Saad Iqbal APIExperts Square for WooCommerce allows Retrieve Embedded Sensitive Data. This issue affects APIExperts Square for WooCommerce: from n/a through 4.7.3.	2026-06-25	8.3	CVE-2026-54848
sahlberg--libnfs	libnfs through 6.0.2 before 935b8db has an xid integer underflow in READ_IOVEC in rpc_read_from_socket in lib/socket.c during a connection to a crafted NFS server, when the expected pdu size exceeds the absolute pdu size from the xid/record-marker.	2026-06-26	7.1	CVE-2026-57918
SALESmanago--SALESmanago & Leadoo	Subscriber SQL Injection in SALESmanago & Leadoo <= 3.11.2 versions.	2026-06-25	8.5	CVE-2026-54822
samuelclay--NewsBlur	NewsBlur before version 14.5.0 contains a server-side request forgery vulnerability in the add_url endpoint that allows authenticated users to make arbitrary server requests to internal networks by failing to filter private IP addresses. Attackers can exploit this to access localhost services and cloud metadata endpoints, enabling internal network scanning and sensitive data exfiltration.	2026-06-25	8.5	CVE-2026-56771
schwehr--libais	libais through 0.15 VdmStream::AddLine uses an unchecked sentinel value as a vector index when processing AIS sentences with empty or out-of-range sequential message IDs. Remote attackers can crash services or vessel systems by sending crafted AIVDM sentences over VHF marine radio or IP feeds, causing out-of-bounds memory access and potential corruption.	2026-06-25	7.5	CVE-2026-56770
Shenzhen Cudy Technology Co., Ltd.--LT300 3.0	Cudy LT300 3.0 running firmware prior to version 2.5.12 contains an OS command injection vulnerability that allows authenticated attackers to execute arbitrary commands by injecting shell metacharacters into the cbid.system.ntp.current POST parameter in the system time configuration interface. Attackers can submit malicious payloads through the NTP	2026-06-26	8.8	CVE-2026-32833

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	settings endpoint to achieve remote code execution on the underlying system.			
Shenzhen i365-Tech Co. Ltd.-- Setracker2 Parental Control App (Android) package com.tgelec.setracker	Setracker2 Android Companion App com.tgelec.setracker versions 3.1.5 and prior only require the password hash when authenticating with backend services from the client. This could allow an attacker, who knows the hash, to authenticate and gain full access.	2026-06-25	8.1	CVE-2026-9222
Shenzhen i365-Tech Co. Ltd.-- Setracker2 Parental Control App (Android) package com.tgelec.setracker	Setracker2 Android Companion App com.tgelec.setracker versions 3.1.5 and prior encrypts requests between the watch and its backend with static hardcoded AES keys and initialization vectors. This allows an attacker to decrypt Setracker2 watch traffic.	2026-06-25	7.5	CVE-2026-9220
Shenzhen i365-Tech Co. Ltd.-- Setracker2 Parental Control App (Android) package com.tgelec.setracker	The Setracker2 Android Companion App (com.tgelec.setracker) versions 3.1.5 and earlier uses MD5 to generate a request signature for authenticating communications between the mobile client and the backend REST API. Attackers could potentially reverse the signature to recover the session ID. With the session ID exposed, an attacker could impersonate the legitimate user and issue authenticated API requests.	2026-06-25	7.5	CVE-2026-9221
Significant-Gravitas-- AutoGPT	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. Prior to 0.6.52, an authenticated user can bypass the SSRF / private-IP protections in SendWebRequestBlock and reach internal network services. _is_ip_blocked() in backend/backend/util/request.py does not normalize IPv4-mapped IPv6 addresses before checking resolved IPs against the blocked IPv4 ranges, and does not block special-use ranges such as 100.64.0.0/10 (CGNAT, RFC 6598). A hostname that resolves to an IPv4-mapped IPv6 address therefore passes validation and the request reaches the embedded internal IPv4 endpoint. This affects all AutoGPT Platform deployments. This vulnerability is fixed in 0.6.52.	2026-06-26	8.5	CVE-2026-56663
Significant-Gravitas-- AutoGPT	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. In versions prior to 0.6.52, the Fill Text Template block is vulnerable to a Denial of Service (DoS) attack. While the backend implements a SandboxedEnvironment to prevent unauthorized attribute access (e.g., blocking __class__), it fails to limit the computational complexity or execution time of the expressions. An attacker can input computationally expensive Python/Jinja2 expressions that consume the server's CPU and memory, leading to a complete system hang or crash. In multi-tenant or self-hosted environments, this results in a complete service outage and "noisy neighbor" effects that require manual administrative intervention to recover. This issue has been fixed in version 0.6.52.	2026-06-24	7.7	CVE-2026-33235
Site Building with Toolset--Toolset Forms	Unauthenticated Insecure Direct Object References (IDOR) in Toolset Forms <= 2.6.24 versions.	2026-06-26	7.5	CVE-2026-56069
siyuan-note-- siyuan	SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, SiYuan contains a stored cross-site scripting (XSS) vulnerability in the Attribute View (database) asset cell renderer that escalates to remote code execution (RCE) in the Electron desktop client. This vulnerability is fixed in 3.7.0.	2026-06-24	9.9	CVE-2026-50551
siyuan-note-- siyuan	SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, CSS snippet body containing </style> breaks out of its surrounding	2026-06-24	9.9	CVE-2026-54067

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	<style> tag when renderSnippet() interpolates it via insertAdjacentHTML. A payload like runs arbitrary JavaScript in the renderer. On Electron desktop builds the renderer runs with nodeIntegration:true, so require('child_process') is reachable from the injected handler and the XSS chains to host RCE. Snippets sync via the workspace repository, so an attacker with write access to any synced workspace plants the payload once and it fires on every device that pulls. The bug also bypasses the user's enabledCSS / enabledJS separation. A user who turned enabledJS off was making a deliberate call not to run untrusted JavaScript; the CSS path runs it anyway. This vulnerability is fixed in 3.7.0.			
siyuan-note--siyuan	SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, the attribute-view (database) cell renderer genAVValueHTML interpolates cell content raw in four of its branches: text, url, phone, and mAsset. A cell value like </textarea> or "> breaks out of its surrounding tag and runs arbitrary JavaScript in the renderer when the victim opens the block-attribute panel. On Electron desktop the renderer runs with nodeIntegration:true, so the XSS chains to host RCE via require('child_process'). AV files live under the workspace and ride normal sync, so an attacker with write access to any synced workspace plants the payload once and it fires on every device that opens a panel containing that row. The kernel doesn't escape on the way in either, so the malicious cell persists byte-for-byte. There's no equivalent of the html.EscapeAttrVal call that protects block IAL attributes at kernel/model/blockial.go:261. This vulnerability is fixed in 3.7.0.	2026-06-24	9.9	CVE-2026-54158
siyuan-note--siyuan	SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, it does not escape the untrusted fields (name, version, author, description) when they are serialized into the data-obj HTML attribute of each marketplace card. Because the attribute is single-quoted and the value is produced with JSON.stringify() (which does not escape ', <, or >), a package whose name contains a single quote breaks out of the attribute and injects arbitrary HTML. In the desktop client the main BrowserWindow runs with nodeIntegration: true, contextIsolation: false, so the injected markup escalates from DOM XSS to arbitrary OS command execution. This is the same root cause and same impact as the original advisory, reached through a sibling sink the patch did not cover. This vulnerability is fixed in 3.7.0.	2026-06-24	9	CVE-2026-55570
siyuan-note--siyuan	SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, the patch for CVE-2026-41894 ("Path Traversal via Double URL Encoding") sanitized the /export/ route but the identical root cause remains in the /assets/*path route. In publish mode (anonymous read-only HTTP endpoint, default port 6808), an unauthenticated remote attacker can read arbitrary files inside WorkspaceDir - including conf/conf.json (which contains the AccessAuthCode SHA256 hash, API token, and sync keys), temp/siyuan.db, temp/blocktree.db, and siyuan.log - by double-URL-encoding .. segments. This vulnerability is fixed in 3.7.0.	2026-06-24	7.5	CVE-2026-54066
siyuan-note--siyuan	SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, renderPackageREADME in kernel/bazaar/readme.go renders a Bazaar package README from Markdown to HTML with the lute engine and SetSanitize(true). The lute sanitizer is an event-handler blacklist: allowAttr rejects only attribute names present in a fixed eventAttrs map copied from the w3schools legacy handler list. That map omits modern event handlers. onpointerover, onpointerdown, onauxclick, onbeforetoggle, onfocusin, onanimationstart, and ontransitionend are not in the list, so the sanitizer passes them through verbatim on any tag. The frontend assigns the rendered HTML to mdElement.innerHTML in app/src/config/bazaar.ts with no client-side DOMPurify on this path, into a normal element in the main document (no iframe, no sandbox). The kernel sends no Content-Security-Policy, X-Frame-Options, or X-Content-Type-Options header on any response, so an inline handler runs when its event	2026-06-24	7.1	CVE-2026-54070

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	fires. The README is rendered when an Administrator opens a package in Settings â†’ Marketplace, after the one-time marketplace trust consent. Install is not required. Result: a third-party Bazaar package author runs JavaScript in the Administrator's authenticated SiYuan origin when the Administrator views and interacts with the package listing, and gains full control of the workspace. This vulnerability is fixed in 3.7.0.			
socat--socat	socat versions 1.8.0.0 through 1.8.1.1 contain a heap-based buffer overflow vulnerability that allows a malicious SOCKS5 proxy server to overwrite adjacent heap memory by exploiting a sign-extension flaw in the DOMAINNAME reply parser. During connection setup, the domain name length byte is read through a signed char field causing a negative bytes_to_read value that is implicitly converted to size_t, resulting in an unbounded heap write into the 262-byte reply buffer with attacker-controlled size and content.	2026-06-25	8.1	CVE-2026-56123
SourceCodester--Class and Exam Timetabling System	A vulnerability was found in SourceCodester Class and Exam Timetabling System 1.0. This affects an unknown function of the file /preview.php. Performing a manipulation of the argument course_year_section results in sql injection. The attack can be initiated remotely. The exploit has been made public and could be used.	2026-06-28	7.3	CVE-2026-13485
SourceCodester--Class and Exam Timetabling System	A vulnerability was determined in SourceCodester Class and Exam Timetabling System 1.0/6.php. This impacts an unknown function of the file /preview6.php. Executing a manipulation of the argument course_year_section can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	2026-06-28	7.3	CVE-2026-13486
SourceCodester--Class and Exam Timetabling System	A vulnerability was identified in SourceCodester Class and Exam Timetabling System 1.0. Affected is an unknown function of the file /archive.php. The manipulation of the argument sy leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	2026-06-28	7.3	CVE-2026-13487
SourceCodester--Class and Exam Timetabling System	A security flaw has been discovered in SourceCodester Class and Exam Timetabling System 1.0/7.php. Affected by this vulnerability is an unknown functionality of the file /preview7.php. The manipulation of the argument course_year_section results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-06-28	7.3	CVE-2026-13488
Spring--Spring Statemachine	Spring Statemachine's Kryo-based persistence backends (JPA, MongoDB, Redis and ZooKeeper) deserialize persisted state-machine contexts without enforcing a class allowlist (CWE-502, deserialisation of untrusted data), which can lead to remote code execution inside the application JVM. Affected versions: Spring Statemachine 4.0.0 through 4.0.1 Spring Statemachine 3.2.0 through 3.2.4	2026-06-23	8.8	CVE-2026-41862
Stranger Studios--Paid Memberships Pro - Add Member From Admin	Unauthenticated Cross Site Request Forgery (CSRF) in Paid Memberships Pro - Add Member From Admin <= 0.7.2 versions.	2026-06-26	8.8	CVE-2026-57659
style-dictionary--style-dictionary	Style Dictionary, a build system for creating cross-platform styles, has a prototype pollution vulnerability starting in version 4.3.0 and prior to version 5.4.4. Impact users have: direct usage of `convertTokenData(tokens, { output: 'object' });`; indirect usage, via using Expand API; and/or indirect usage via SD's transform lifecycle. Impact is high for this when style-dictionary is used as an integration in a NodeJS server application. Impact is moderate for when style-dictionary is used as an integration in a Web application. Impact is low for most common cases where the user of style-dictionary also maintains the tokens, and access is limited via read/write access to the repository/workflows where it is used. A patch has been published in version `5.4.4`. The only known workaround is to sanitize token data first. Whether using DTCG format or old Style	2026-06-24	8.8	CVE-2026-54639

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Dictionary format, check the token data object recursively for any object keys that include `__proto__`.			
StylemixThemes--Motors	Unauthenticated Broken Access Control in Motors <= 1.4.109 versions.	2026-06-25	7.5	CVE-2026-54828
StylemixThemes--Splash - Sport Club WordPress Theme for Basketball, Football, Hockey	Contributor Local File Inclusion in Splash - Sport Club WordPress Theme for Basketball, Football, Hockey <= 4.4.3 versions.	2026-06-26	7.5	CVE-2025-68063
SureCart--SureCart	Unauthenticated Cross Site Scripting (XSS) in SureCart <= 4.3.2 versions.	2026-06-26	7.1	CVE-2026-57314
Syed Balkhi--Intranet & Private Site All-In-One Intranet	Unauthenticated Broken Access Control in Intranet & Private Site – All-In-One Intranet <= 1.8.1 versions.	2026-06-26	7.5	CVE-2026-54837
TablePress--TablePress	Unauthenticated Cross Site Scripting (XSS) in TablePress <= 3.3.1 versions.	2026-06-25	7.1	CVE-2026-56051
teableio--teable	Teable's v2 REST API controller lacks @Permissions metadata on ORPC endpoints, allowing any authenticated user to bypass authorization checks. Attackers can read table schemas, create tables, and modify or delete records across bases and tables via endpoints like GET /api/v2/tables/get and POST /api/v2/tables/updateRecords.	2026-06-26	8.8	CVE-2026-56773
Templatespare--TemplateSpare	Administrator Arbitrary File Upload in TemplateSpare <= 4.2.0 versions.	2026-06-26	9.1	CVE-2026-57658
tenable--Tenable Identity Exposure	Tenable Identity Exposure contains multiple unauthenticated API endpoints under /w/api/* that expose sensitive application configuration data including cleartext LDAP credentials, SAML configuration, user accounts, and directory settings to unauthenticated remote attackers. Affected responses are served with Cache-Control: public headers and without Vary: Cookie, allowing reverse proxies and CDNs to cache and serve sensitive data to unauthenticated users even after authentication is applied.	2026-06-23	7.5	CVE-2026-13007
Tenda--JD12L	A security vulnerability has been detected in Tenda JD12L 16.03.53.23. Impacted is the function formSetPptpServer of the file /goform/SetPptpServerCfg. Such manipulation of the argument startIp leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used.	2026-06-28	8.8	CVE-2026-13515
Tenda--JD12L	A vulnerability was detected in Tenda JD12L 16.03.53.23. The affected element is the function fromSetWifiGusetBasic of the file /goform/WifiGuestSet. Performing a manipulation of the argument shareSpeed results in stack-based buffer overflow. The attack may be initiated remotely. The exploit is now public and may be used.	2026-06-28	8.8	CVE-2026-13516
ThemeCatcher--Quform	Subscriber Arbitrary File Upload in Quform <= 2.23.0 versions.	2026-06-26	9.9	CVE-2026-56058
Themefic--Tourfic	Subscriber SQL Injection in Tourfic <= 2.22.5 versions.	2026-06-26	8.5	CVE-2026-56064
themefic--Tourfic AI Powered Travel Booking, Hotel Booking & Car Rental WordPress Plugin	The Tourfic - AI Powered Travel Booking, Hotel Booking & Car Rental WordPress Plugin plugin for WordPress is vulnerable to generic SQL Injection via the 'post_id' parameter in all versions up to, and including, 2.22.7 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The AJAX handler is registered for unauthenticated users via wp_ajax_nopriv_tf_room_availability, and the required nonce is emitted on the public single-hotel page template,	2026-06-25	7.5	CVE-2026-12937

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allowing unauthenticated attackers to freely obtain a valid nonce and reach the vulnerable code path.			
ThemeFusion--Fusion Builder	Contributor Privilege Escalation in Fusion Builder <= 3.15.4 versions.	2026-06-26	8.8	CVE-2026-56008
ThemeHunk--Advance Product Search	Unauthenticated SQL Injection in Advance Product Search <= 1.4.4 versions.	2026-06-26	9.3	CVE-2026-56070
themewant--Easy Elements for Elementor " Addons & Website Templates	Unauthenticated Privilege Escalation in Easy Elements for Elementor – Addons & Website Templates <= 1.4.9 versions.	2026-06-26	9.8	CVE-2026-56028
Tomdever--wpForo Forum	Contributor SQL Injection in wpForo Forum <= 3.0.9 versions.	2026-06-26	8.5	CVE-2026-57636
tomojitakasu--RTKLIB	RTKLIB through 2.4.3 contains an out-of-bounds write vulnerability in decode_type1033 function that fails to clamp length counters to destination buffer size, allowing up to 191-byte overflow into fixed 64-byte descriptor fields. An attacker controlling an NTRIP or serial RTCM3 correction stream can craft a valid CRC-bearing type-1033 message to corrupt adjacent rtcn_t object members, potentially achieving arbitrary code execution or denial of service.	2026-06-25	9.8	CVE-2026-56786
ToolJet--ToolJet	ToolJet is the open-source foundation am AI-native platform for building and deploying internal tools, workflows and AI agents. Prior to 3.20.178-lts, there's an SSRF in the RestAPI data source component. The RestAPI data source executes HTTP requests server-side, and its private IP filter only checks the hostname string - not the resolved IP. DNS names like 169.254.169.254.nip.io resolve to the Azure IMDS link-local address and bypass the filter entirely. This allows any authenticated user (free tier) to steal Azure managed identity tokens for the AKS production cluster. This vulnerability is fixed in 3.20.178-lts.	2026-06-25	8.3	CVE-2026-55412
Traefik--Traefik	Traefik before 2.10.5 and 3.0.0-beta4 is affected by a denial-of-service vulnerability in HTTP/2 request handling inherited from the Go standard library's HTTP/2 implementation (CVE-2023-44487 / CVE-2023-39325, the 'Rapid Reset' technique). A remote attacker can rapidly create and cancel HTTP/2 streams to exhaust server resources and cause service unavailability.	2026-06-23	7.5	CVE-2023-54365
Tribulant Software--Newsletters	newsletters_subscribers Broken Access Control in Newsletters <= 4.13 versions.	2026-06-26	8.1	CVE-2026-57645
Tribulant Software--Newsletters	Unauthenticated Broken Access Control in Newsletters <= 4.13 versions.	2026-06-26	7.3	CVE-2026-54840
TryGhost--Ghost	Ghost is a Node.js content management system. From until 6.37.0, when Ghost is behind a shared caching layer that results in cached content being shared between different visitors, an unauthenticated user could send an x-ghost-preview header that altered the rendered frontend response. In affected cache configurations, that response could be stored and served to subsequent visitors requesting the same page, allowing cache poisoning of request-specific preview output. When running Ghost's frontend and admin panel on the same domain this could be used to take over staff user accounts. When running these on different domains staff accounts have no exposure. This vulnerability is fixed in 6.37.0.	2026-06-24	9.6	CVE-2026-53943
TryGhost--Ghost	@tryghost/activitypub is Ghost's social/federation client app. Prior to 3.1.0, the ActivityPub client in Ghost was vulnerable to JavaScript injection on posts shared by a maliciously customised ActivityPub server. This vulnerability is fixed in 3.1.0.	2026-06-24	7.5	CVE-2026-53950
twentyhq--twenty	Twenty is an open-source CRM (customer relationship management) platform. Prior to 2.9.0, Twenty was vulnerable to a cross-workspace	2026-06-24	7.6	CVE-2026-55583

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	insecure direct object reference (IDOR) in the AI agent monitor's AgentTurnResolver, in packages/twenty-server/src/engine/metadata-modules/ai/ai-agent-monitor/resolvers/agent-turn.resolver.ts. The agentTurns(agentId) query and the evaluateAgentTurn(turnId) mutation looked up rows by agentId or id only; although AgentTurnEntity has a workspaceId column, it was not included in the WHERE clause, and the class-level guards only checked that the caller was authenticated in some workspace rather than that the requested object belonged to it, with the same flaw present in agent-turn-grader.service.ts. As a result, any authenticated user with the AI settings flag, a workspace owner by default, could target any other workspace on the same instance given the victim's agentId or turnId: agentTurns returned the victim's full chat history including message parts such as raw chat text, tool calls, and tool outputs, while evaluateAgentTurn inserted an agentTurnEvaluation row with the victim's workspaceId and fed the victim's turn into the default LLM. The agentId and turnId are non-guessable UUIDs but are exposed in the URL of the settings page. This issue is fixed in version 2.9.0.			
Tyche Softwares-- Abandoned Cart Pro for WooCommerce	Subscriber Privilege Escalation in Abandoned Cart Pro for WooCommerce <= 10.4.0 versions.	2026-06-26	8.8	CVE-2026-56010
tychesoftwares-- Print Invoice & Delivery Notes for WooCommerce	Unauthenticated Sensitive Data Exposure in Print Invoice & Delivery Notes for WooCommerce <= 7.1.1 versions.	2026-06-26	7.5	CVE-2026-56060
Ubuntu-- Canonical ADSys	An issue was discovered in Canonical ADSys upstream versions through v0.16.2. During Active Directory Certificate Services (AD CS) certificate auto-enrollment via the vendored Samba client script (internal/policies/certificate/python/vendor_samba/gp/gp_cert_auto_enroll_ext.py), ADSys utilizes a plaintext HTTP connection (http://) instead of a secure HTTPS connection (https://) to request the CA certificate from the Active Directory Certificate Services server (GetCACert). An unauthenticated network attacker positioned between the managed Ubuntu host and the configured AD CS CA hostname can conduct a Man-in-the-Middle (MITM) attack. By intercepting the plaintext HTTP request, the attacker can supply an arbitrary, attacker-controlled Root CA certificate. Because the system automatically accepts this certificate and registers it into the local system trust store via update-ca-certificates, this results in system-wide trust store poisoning. Consequently, TLS clients utilizing the operating system trust store on the affected machine will accept rogue certificates for arbitrary domains, enabling persistent decryption and interception of subsequent TLS connections. This issue is resolved in version v0.16.3.	2026-06-22	8.3	CVE-2026-12249
ultimatemember--Ultimate Member User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin	The Ultimate Member plugin for WordPress is vulnerable to Account Takeover via Password Reset Link Disclosure in all versions up to and including 2.11.4. This is due to a chain of three logic bugs: (1) an MD5 hash fallback in get_directory_by_hash() that allows any post to be used as a member directory by computing SUBSTRING(MD5(post_id), 11, 5), (2) a strpos() parsing logic flaw in post_data() that allows bypassing WordPress's protected meta key restrictions by placing '_um_' anywhere in the meta key name rather than at the start, and (3) missing field name validation in build_user_card_data() that allows arbitrary field names including 'password_reset_link' to be passed to um_filtered_value(). This makes it possible for authenticated attackers with Contributor-level access and above to create a malicious post via XMLRPC with crafted meta fields, use the MD5 fallback to point the member directory AJAX handler to their post, inject 'password_reset_link' into the tagline_fields configuration, and	2026-06-24	8.8	CVE-2026-7761

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	leak live password reset URLs for all users in the member directory response, including administrators.			
Uncanny Owl-- Uncanny Automator	Unauthenticated PHP Object Injection in Uncanny Automator <= 7.3.1.2 versions.	2026-06-26	8.1	CVE-2026-56031
Uncanny Owl-- Uncanny Automator Pro	Subscriber PHP Object Injection in Uncanny Automator Pro <= 7.3.0.6 versions.	2026-06-26	9.8	CVE-2026-56057
unclecode-- crawl4ai	Crawl4AI is an open-source LLM friendly web crawler & scraper. Prior to 0.8.7, the <code>_safe_eval_expression()</code> function in the computed fields feature uses an AST validator that only blocks attributes starting with underscore. Python generator and frame object attributes (<code>gi_frame</code> , <code>f_back</code> , <code>f_builtins</code>) do NOT start with underscore, enabling a complete sandbox escape to achieve arbitrary code execution. The attack requires no authentication (JWT disabled by default) and is triggered via POST <code>/crawl</code> with a crafted extraction schema. This vulnerability is fixed in 0.8.7.	2026-06-23	9.8	CVE-2026-53753
unclecode-- crawl4ai	Crawl4AI is an open-source LLM friendly web crawler & scraper. Prior to 0.8.9, the Docker API server applied its SSRF destination check to the crawl target URL only, not to the proxy address. An unauthenticated request could supply a proxy pointing at an internal IP and route the browser through it, reaching internal services and cloud-metadata endpoints, while using a perfectly valid crawl URL. The Docker API is unauthenticated by default. <code>/crawl</code> , <code>/crawl/stream</code> , and <code>/crawl/job</code> accept a <code>browser_config</code> (and <code>crawler_config</code>). The following all feed Chromium's egress and were unchecked: <code>browser_config.proxy_config.server</code> , <code>browser_config.proxy</code> (deprecated field), <code>crawler_config.proxy_config.server</code> , and <code>--proxy-server / --proxy-pac-url / --proxy-bypass-list / --host-resolver-rules</code> flags in <code>browser_config.extra_args</code> . This vulnerability is fixed in 0.8.9.	2026-06-23	8.6	CVE-2026-53755
unclecode-- crawl4ai	Crawl4AI is an open-source LLM friendly web crawler & scraper. Prior to 0.8.8, the Docker API server's SSRF protection (<code>validate_webhook_url / validate_url_destination</code> in <code>deploy/docker/utls.py</code>) used an explicit IPv4/IPv6 CIDR blocklist that missed several address families. An attacker could reach internal services and cloud metadata endpoints (e.g. 169.254.169.254) despite the filter by encoding an internal IPv4 address inside an IPv6 transition form, or by using the IPv6 unspecified address. Because the Docker API is unauthenticated by default (<code>jwt_enabled: false</code>), no credentials are required. This vulnerability is fixed in 0.8.8.	2026-06-23	7.5	CVE-2026-53754
ValvePress-- Automatic	Unauthenticated Cross Site Scripting (XSS) in Automatic < 3.135.1 versions.	2026-06-26	7.1	CVE-2026-56045
vanhauser-thc-- thc-hydra	Hydra through 9.7, fixed in commit 9cc84c2, contains a stack buffer overflow in NTLM authentication across SMTP, POP3, IMAP, NNTP, HTTP, HTTP-Proxy, and HTTP-Proxy-Urlenum modules when processing malicious NTLM Type-2 challenges. A malicious server can send a crafted NTLM Type-2 challenge with an excessively long domain string, causing base64-encoded response data to overflow a 500-byte stack buffer by 18 to 330 bytes, enabling remote code execution on systems without stack protection.	2026-06-25	8.8	CVE-2026-56766
vllm-project-- vllm	vLLM is an inference and serving engine for large language models (LLMs). From 0.3.0 until 0.22.0, a vulnerability in ASGI web servers and starlette's trust on those web servers enables an authentication bypass of the OpenAI API AuthenticationMiddleware. It allows to use the API without providing the configured <code>VLLM_API_KEY</code> or <code>--api-key</code> . This vulnerability is fixed in 0.22.0.	2026-06-22	9.1	CVE-2026-48746
vllm-project-- vllm	vLLM is an inference and serving engine for large language models (LLMs). Prior to 0.22.1, the vLLM Dockerfile is vulnerable to a dependency confusion attack through the <code>flashinfer-jit-cache</code> package. The package is installed from a custom index (<code>flashinfer.ai/whl/</code>) using <code>--extra-index-url</code> , but the package name was not registered on PyPI, and <code>UV_INDEX_STRATEGY="unsafe-best-match"</code> is set globally. An attacker	2026-06-22	8.8	CVE-2026-54232

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	who registers flashinfer-jit-cache on PyPI with version 0.6.11.post2 can execute arbitrary code as root during the Docker build and backdoor every resulting container image, enabling exfiltration of all user prompts, API credentials, and model data from production vLLM deployments This vulnerability is fixed in 0.22.1.			
vllm-project--vllm	vLLM is an inference and serving engine for large language models (LLMs). Prior to 0.22.0, an assert-based security check in vLLM's activation function loading allows any unauthenticated attacker to achieve arbitrary code execution on the server by publishing a malicious HuggingFace model, when vLLM runs in Python optimized mode (python -O or PYTHONOPTIMIZE=1). This vulnerability is fixed in 0.22.0.	2026-06-22	7.5	CVE-2026-41523
vtk--vtk	vtk vtk-dicom vtkDICOMItem::NewDataElement heap-based buffer overflow vulnerability	2026-06-25	8.1	CVE-2026-22879
warpdotdev--warp	Warp is an agentic development environment. From 0.2023.10.24.08.03.stable_00 until 0.2026.05.06.15.42.stable_01, Warp may open executable local files through the operating system default file handler. A malicious Markdown document or project can contain a local-file link that appears as normal rendered content. If a user opens the Markdown in Warp and clicks the link, affected builds may route the resolved local file to a platform file opener instead of limiting the action to safe viewer/editor targets. This vulnerability is fixed in 0.2026.05.06.15.42.stable_01.	2026-06-24	8.8	CVE-2026-48704
warpdotdev--warp	Warp is an agentic development environment. From 0.2025.08.06.08.12.stable_00 until 0.2026.05.06.15.42.stable_01, Warp contains a command injection in the prompt branch selector. A user who can publish a branch to a Git repository opened in Warp can cause a crafted branch name to be interpreted by the victim's shell if the victim selects that branch from the UI. This vulnerability is fixed in 0.2026.05.06.15.42.stable_01.	2026-06-24	8	CVE-2026-48719
warpdotdev--warp	Warp is an agentic development environment. From 0.2025.03.05.08.02.stable_00 until 0.2026.05.06.15.42.stable_01, Warp accepts non-inline `OSC 1337;File` payloads from terminal output and materialize the decoded payload as a local file without an additional confirmation step. This vulnerability is fixed in 0.2026.05.06.15.42.stable_01.	2026-06-24	8.8	CVE-2026-48720
warpdotdev--warp	Warp is an agentic development environment. From 0.2025.10.08.08.12.stable_00 until 0.2026.05.06.15.42.stable_01, Warp contains a command execution permission-check bypass in the default unsandboxed CLI agent profile. The CLI profile is non-interactive and relies on a command denylist as a safety boundary for commands that should require confirmation. Because command strings were checked before canonicalizing leading environment-variable assignments, an attacker who can influence the agent's command output may cause denylisted commands to be treated as non-denylisted. This vulnerability is fixed in 0.2026.05.06.15.42.stable_01.	2026-06-24	8.6	CVE-2026-48721
warpdotdev--warp	Warp is an agentic development environment. From 0.2021.04.25.23.05.stable_00 until 0.2026.05.06.15.42.stable_01, Warp allows terminal output to request access to the local system clipboard. A malicious remote host, remote program, or other attacker-controlled terminal output source can trigger clipboard reads or writes without a separate confirmation step. This crosses the trust boundary between untrusted terminal output and the user's local desktop clipboard. This vulnerability is fixed in 0.2026.05.06.15.42.stable_01.	2026-06-24	8.1	CVE-2026-48725
warpdotdev--warp	Warp is an agentic development environment. From 0.2023.03.21.08.02.stable_00 until 0.2026.05.06.15.42.stable_01, Warp contains a command injection issue in the legacy SSH background command path. Warp used the remote working directory reported by the session when building helper commands for SSH-backed metadata collection. A remote host, repository, or directory name controlled by an	2026-06-24	8.8	CVE-2026-48732

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker could cause that helper command to execute additional shell syntax on the remote host as the victim's authenticated SSH account. This vulnerability is fixed in 0.2026.05.06.15.42.stable_01.			
warpdotdev--warp	Warp is an agentic development environment. From 0.2025.04.09.08.11.stable_00 until 0.2026.05.06.15.42.stable_01, Warp contains a command execution policy bypass in Agent code search tools. The affected Grep and FileGlob actions are authorized as read/search operations, but their implementations build shell command strings from Agent-controlled inputs (search text, paths, glob patterns) and execute them in the active terminal session. This vulnerability is fixed in 0.2026.05.06.15.42.stable_01.	2026-06-24	7.8	CVE-2026-48703
warpdotdev--warp	Warp is an agentic development environment. From 0.2024.02.20.08.01.stable_01 until 0.2026.05.06.15.42.stable_01, Warp contains a command injection issue in the Linux external editor launcher. Warp expanded freedesktop .desktop Exec templates for affected editor integrations and executed the expanded command through a shell. A user who opens an attacker-controlled local file path through an affected external editor or system-default editor route can cause shell syntax embedded in that path to execute as the local user. This vulnerability is fixed in 0.2026.05.06.15.42.stable_01.	2026-06-24	7.8	CVE-2026-48731
warpdotdev--warp	Warp is an agentic development environment. From 0.2024.03.12.08.02.stable_01 until 0.2026.05.06.15.42.stable_01, Warp contains an OS command injection vulnerability in the WSL URL-opening fallback. When Warp is running under WSL and cannot open a URL through wslview, it falls back to a Windows command processor path. A URL controlled through terminal output can reach that fallback when the user opens the link. This vulnerability is fixed in 0.2026.05.06.15.42.stable_01.	2026-06-24	7.7	CVE-2026-54699
Wasiliy Strecker--Contest Gallery	Contributor SQL Injection in Contest Gallery <= 30.0.0 versions.	2026-06-26	8.5	CVE-2026-57662
webp-sh--webp_server_go	WebP Server Go through 0.14.4 contains a path traversal vulnerability on Windows that allows unauthenticated attackers to read files outside the configured IMG_PATH directory by sending requests with percent-encoded backslashes (%5C) that bypass the path.Clean() sanitization in handler/router.go. Attackers can exploit the discrepancy between Go's forward-slash-only path normalization and Windows file system APIs that treat backslashes and forward slashes as equivalent to access arbitrary files on the host filesystem accessible to the server process.	2026-06-22	7.5	CVE-2026-53779
wedevs--Dokan Pro	The Dokan Pro plugin for WordPress is vulnerable to time-based SQL Injection via the via 'latitude' and 'longitude' parameters in all versions up to, and including, 5.0.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-06-25	7.5	CVE-2026-12077
weDevs--weMail	Unauthenticated Cross Site Scripting (XSS) in weMail <= 2.1.2 versions.	2026-06-26	7.1	CVE-2026-57322
withastro--astro	Astro is a web framework. Prior to 6.3.3, when a component uses a client:* directive, Astro inserts named slot content into a data-astro-template attribute without HTML escaping the slot name allowing an attacker to break out of the attribute context and inject arbitrary HTML, resulting in reflected XSS during SSR. This vulnerability is fixed in 6.3.3.	2026-06-22	7.1	CVE-2026-50146
withastro--astro	Astro is a web framework. Prior to 6.4.6, Astro SSR apps with prerendered error pages (/404 or /500 using export const prerender = true) fetch those pages over HTTP at runtime when an error occurs. The URL for this fetch is derived from request.url, which in turn gets its origin from the incoming Host header. When the Host header is not validated against allowedDomains, an attacker can point the fetch at an arbitrary host and read the response. This vulnerability is fixed in 6.4.6.	2026-06-22	7.5	CVE-2026-54299

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WordPress.com--Gutenverse Form	Unauthenticated Cross Site Scripting (XSS) in Gutenverse Form <= 2.4.7 versions.	2026-06-26	7.1	CVE-2026-56040
WordPress.com--Quick Interest Slider	Unauthenticated Cross Site Scripting (XSS) in Quick Interest Slider <= 3.1.6 versions.	2026-06-26	7.1	CVE-2026-56039
WP All Import--WP All Import	Administrator SQL Injection in WP All Import <= 4.0.1 versions.	2026-06-26	7.6	CVE-2026-57628
WP Swings--Subscriptions for WooCommerce	Unauthenticated Broken Access Control in Subscriptions for WooCommerce <= 1.9.5 versions.	2026-06-26	7.5	CVE-2026-56061
wpDataTables--wpDataTables	Unauthenticated SQL Injection in wpDataTables <= 7.4 versions.	2026-06-26	9.3	CVE-2026-54825
wpeverest--Everest Forms	Unauthenticated Cross Site Scripting (XSS) in Everest Forms <= 3.4.8 versions.	2026-06-26	7.1	CVE-2026-57312
wpjobportal--WP Job Portal	Contributor SQL Injection in WP Job Portal <= 2.5.2 versions.	2026-06-26	8.5	CVE-2026-57653
WPMU DEV--Forminator	Unauthenticated Cross Site Scripting (XSS) in Forminator <= 1.53.1 versions.	2026-06-25	7.1	CVE-2026-56071
WSO2--WSO2 API Manager	The WSO2 API Manager's message flow component, when processing WS-Addressing headers, does not sufficiently validate or restrict user-controlled input within these headers. This omission allows an attacker to manipulate WS-Addressing headers to specify arbitrary destinations for server-initiated requests. Successful exploitation allows an unauthenticated attacker to control the destination of server-initiated requests originating from the WSO2 API Manager. This direct control can enable unauthorized access to internal network resources or services that would typically be inaccessible from external networks.	2026-06-26	8.3	CVE-2026-2053
Xtemos--WoodMart	Unauthenticated Cross Site Scripting (XSS) in WoodMart <= 8.5.3 versions.	2026-06-26	7.1	CVE-2026-56072
yashpokharna2555--restaurent-management-system	A vulnerability was identified in yashpokharna2555 restaurent-management-system. This affects an unknown function of the file /forgotpassword.php of the component POST Parameter Handler. Such manipulation of the argument email leads to sql injection. The attack can be launched remotely. The exploit is publicly available and might be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-28	7.3	CVE-2026-13498
YMC--YMC Filter	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in YMC Filter allows SQL Injection. This issue affects YMC Filter: from n/a through 3.11.5.	2026-06-25	9.3	CVE-2026-54836
yt-dlp--yt-dlp	yt-dlp is a command-line audio/video downloader. Prior to 2026.06.09, a vulnerability exists in yt-dlp that allows a remote attacker to write arbitrary OS-shortcut files (such as .desktop, .url, .webloc) to the user's filesystem, bypassing the remediation for CVE-2024-38519. The allowlist explicitly included the unsafe extensions .desktop, .url, and .webloc so that the functionality of the --write-link option (and its variants) could be preserved. These allowlist inclusions can be exploited by an attacker to write malicious OS-shortcut files in the context of a media or subtitles download. This vulnerability is fixed in 2026.06.09.	2026-06-23	8.3	CVE-2026-50023
yt-dlp--yt-dlp	yt-dlp is a command-line audio/video downloader. Prior to 2026.06.09, if aria2c is used as an external downloader for a fragmented manifest format (such as an HLS/DASH stream), yt-dlp passes insufficiently sanitized input to aria2c that allows an attacker to perform an arbitrary file write. On Windows platforms, this can lead to immediate arbitrary code execution. On non-Windows platforms, this can lead to arbitrary code execution upon the next invocation of yt-dlp. This vulnerability is fixed in 2026.06.09.	2026-06-23	8.3	CVE-2026-50574

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zaproxy--zap-extensions	Zed Attack Proxy (ZAP) ViewState add-on before version 4 contains an insecure deserialization vulnerability that allows attackers who control a proxied web server to achieve arbitrary code execution by embedding a malicious serialized Java object in the javax.faces.ViewState HTTP response parameter. The JSFViewState.decode() method base64-decodes the ViewState value and passes it directly to ObjectInputStream.readObject() without a deserialization filter, allowlist, or type restriction, causing the malicious object to be deserialized within the ZAP JVM when the Desktop UI renders the ViewState panel.	2026-06-26	8.8	CVE-2026-57527
zephyrproject--zephyr	Zephyr's IP socket recvmsg() implementation (subsys/net/lib/sockets/sockets_inet.c, insert_pktinfo()) validated the user-supplied ancillary (msg_control) buffer using only the payload length (msg-msg_controllen < pktinfo_len) before writing a full control message consisting of an aligned cmsg header plus the payload. Because the check omitted the cmsg header size, a control buffer whose length falls in the under-checked window (e.g. 16-27 bytes for IPv4 IP_PKTINFO on a 64-bit target, where a single element actually occupies 28 bytes) passes the guard yet causes a fixed-size out-of-bounds write of up to one cmsg header (~12 bytes) past the end of the buffer. Under CONFIG_USERSPACE the recvmsg verifier allocates a kernel-heap copy of the control buffer sized to msg_controllen and runs the implementation against it, so the overflow corrupts kernel heap memory and is triggerable from an unprivileged userspace thread; in supervisor mode it corrupts the caller's buffer. The path is reachable on a UDP/IP socket with IP_PKTINFO/IPv6_RECVPKTINFO (or hoplimit/timestamping) enabled when the application calls recvmsg() with an undersized control buffer and a datagram is received; part of the overwritten bytes (the destination IP in ipi_addr) is influenced by the received packet. The fix makes the capacity check use NET_CMSG_SPACE(pktinfo_len) (aligned header + aligned data) and returns -ENOMEM when the buffer is too small. Affected: v3.6.0 through v4.4.0.	2026-06-27	8.7	CVE-2026-10643
zephyrproject--zephyr	Zephyr's BSD-sockets getaddrinfo() implementation (subsys/net/lib/sockets/getaddrinfo.c) passes a pointer to a stack-allocated state object (struct getaddrinfo_state ai_state) as the user_data of an asynchronous DNS resolver query. The socket layer waits on a semaphore with a timeout deliberately set slightly longer than the resolver's own per-query timeout. When that semaphore wait nonetheless times out (-EAGAIN) - which can occur when the resolver's timeout work is delayed by workqueue contention, or in the documented multi-retry configuration where CONFIG_NET_SOCKETS_DNS_TIMEOUT exceeds CONFIG_NET_SOCKETS_DNS_BACKOFF_INTERVAL - the pre-fix code retries the query (goto again) without cancelling the previous one and without resetting the semaphore. The previous query slot remains active in the resolver with its callback and the stack pointer as user_data, and ai_state_dns_id is overwritten so the stale query can no longer be cancelled. A subsequent DNS response delivered over UDP and matched by its 16-bit transaction id (in dispatcher_cb()/dns_read()), or the resolver's own delayed query-timeout work, then invokes dns_resolve_cb() against the now out-of-scope stack frame, writing through the stale pointer (state-status, state-idx, state-ai_arr[], and k_sem_give()). Because the triggering response is network-delivered and its 16-bit id is spoofable/replayable by an on- or off-path attacker, this is a network-influenceable use-after-return that can corrupt reused stack memory, leading to crashes/denial of service or memory corruption. The fix cancels the timed-out query by name and type before retrying and resets the local semaphore, eliminating the stale callback path. Affected: Zephyr v4.0.0 through v4.4.0.	2026-06-28	7.4	CVE-2026-10646
zephyrproject--rtos--Zephyr	A malformed Bluetooth Classic SDP attribute can trigger a reachable assertion in Zephyr's SDP parser. In subsys/bluetooth/host/classic/sdp.c, bt_sdp_parse_attribute() accepts an input buffer once it contains the 1-	2026-06-22	7.1	CVE-2026-10651

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	byte attribute type and 2-byte attribute id, but then unconditionally pulls an additional byte for the value type without verifying that the byte is present. A truncated 3-byte attribute (for example 09 00 09) therefore reaches net_buf_simple_pull() with insufficient remaining length, triggering the __ASSERT_NO_MSG(buf->len >= len) check and a kernel panic in assert-enabled builds (denial of service). In builds where assertions are disabled, parsing may continue past the end of the available buffer, leading to an out-of-bounds read and undefined behavior.			
zephyrproject-rtos--Zephyr	A missing length validation in the Zephyr Bluetooth Host ISO receive path can be triggered by malformed HCI ISO data. In bt_iso_rcv() (subsys/bluetooth/host/iso.c), when processing PB=START/SINGLE fragments, the code pulls a TS SDU header (8 bytes, ts=1) or a non-TS SDU header (4 bytes, ts=0) without first verifying that buf->len contains at least that many bytes. The outer HCI ISO length check in hci_iso() validates payload length consistency but not the minimum inner SDU header size, so a packet with payload length 1 passes hci_iso() and then reaches net_buf_pull_mem(), which asserts buf->len >= len. As a result, malformed ISO traffic deterministically triggers a kernel assert (denial of service) in assert-enabled builds, and in non-assert builds the same path may proceed with an undersized buffer, leading to out-of-bounds read behavior. The issue affects products using the Zephyr Host with CONFIG_BT_ISO_RX enabled, particularly where incoming HCI data can be influenced by a malicious or compromised controller or malformed forwarded ISO traffic.	2026-06-22	7.1	CVE-2026-10658
zephyrproject-rtos--Zephyr	Zephyr's IPv6 network stack can be prevented from receiving or processing future incoming packets by sending a small number of maliciously fragmented IPv6 packets. When such a packet is handled by the fragment-header processing path, the associated RX network packet buffer (allocated from a memory slab) is not released back to the pool. Repeating the malicious packet exhausts all RX buffer slots, after which the device can no longer obtain RX buffers and stops receiving traffic, resulting in a denial of service.	2026-06-25	7.5	CVE-2026-13351
zohocorp--manageengine_adselfservice_plus	In ManageEngine ADSelfService Plus, RecoveryManager Plus, M365 Manager Plus, and ADAudit Plus, the SSO tickets generated to authenticate that session could be predicted by an unauthenticated user, leading to account takeover.	2026-06-23	9	CVE-2026-11374
@fastify/express -- @fastify/express	@fastify/express versions 4.0.6 and earlier only rewrite the plugin prefix for middleware mount paths when the path argument is a string. Non-string mount paths (arrays of paths and regular expressions) are left unprefix inside prefixed plugin scopes, so middleware registered with those forms does not match the actual prefixed request path. Applications that use path-scoped middleware for authentication, authorization, rate limiting, or auditing on routes inside a prefixed scope can be bypassed by sending a request to the prefixed route, because Fastify still matches the route but the middleware is skipped. Patches: upgrade to @fastify/express 4.0.7. Workarounds: use string mount paths instead of arrays or regular expressions in prefixed plugins, or register one use call per path.	2026-06-30	9.1	CVE-2026-6556
@fastify/middie -- @fastify/middie	@fastify/middie versions 9.1.0 through 9.3.2 decode the encoded slash %2F inside path parameter values before matching middleware paths, while Fastify's underlying router preserves the encoding during route lookup. The two layers disagree on the canonical request path, so the middleware fails to match a URL that the route handler does match. When middleware is used for authentication, authorization, rate limiting, or auditing on parameterized paths, an attacker can reach the protected handler by sending a single crafted URL with an encoded slash in the parameter position. The bypass is HTTP method agnostic and requires no authentication or special preconditions. Patches: upgrade to @fastify/middie 9.3.3. Workarounds: avoid parameterized middleware paths for security decisions, or enforce authentication at the route handler or via a Fastify hook that runs after the router has resolved the request.	2026-07-01	9.1	CVE-2026-14198

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
@fastify/middie--@fastify/middie	@fastify/middie versions 9.1.0 through 9.3.2 fail to guard the URL normalization step used by the standalone engine when incoming request paths contain malformed percent-encoded sequences. Inputs such as an incomplete percent escape or a truncated multibyte sequence cause the underlying decoder to throw synchronously, and the exception escapes the middie normalize step and terminates the Node.js process. The bypass affects applications that call middie.run directly on the standalone engine API, causing an immediate denial of service for all connected clients until restart. Applications using the Fastify plugin path are not affected because Fastify's error handler catches the exception. Patches: upgrade to @fastify/middie 9.3.3. Workarounds: migrate from the standalone engine API to the Fastify plugin path, where the framework error handler catches the exception.	2026-07-01	7.5	CVE-2026-14181
a--nicen-localize-image	Contributor SQL Injection in nicen-localize-image <= 1.4.9 versions.	2026-07-02	8.5	CVE-2026-57756
acl project--acl	acl before version 2.4.0 contains a symlink traversal vulnerability in the libacl pathname-based functions acl_get_file(), acl_set_file(), acl_extended_file(), and acl_delete_def_file() that allows local attackers to escalate privileges by replacing any pathname component with a symbolic link. Attackers who control any component of a pathname processed by a privileged caller can redirect ACL read or write operations to arbitrary files or directories, enabling unauthorized manipulation of access control lists and local privilege escalation.	2026-06-29	7.1	CVE-2026-54369
Adobe--Adobe Campaign Classic (ACC)	Adobe Campaign Classic (ACC) versions 7.4.3 build 9396 and earlier are affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-30	10	CVE-2026-48286
Adobe--ColdFusion	ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-30	10	CVE-2026-48276
Adobe--ColdFusion	ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-30	10	CVE-2026-48277
Adobe--ColdFusion	ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-30	10	CVE-2026-48281
Adobe--ColdFusion	ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-30	10	CVE-2026-48282
Adobe--ColdFusion	ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-30	10	CVE-2026-48283
Adobe--ColdFusion	ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read and limited write access. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-30	9.3	CVE-2026-48313
Adobe--ColdFusion	ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code	2026-06-30	9.3	CVE-2026-48315

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execution in the context of the current user. An attacker could exploit this vulnerability to inject malicious scripts into a web page, potentially gaining elevated access or control over the victim's account or session. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.			
Adobe--ColdFusion	ColdFusion versions 2025.9, 2023.20 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-30	8.6	CVE-2026-48285
Adobe--ColdFusion	ColdFusion versions 2025.9, 2023.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this vulnerability to inject malicious scripts into a web page, potentially resulting in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious link. Scope is changed.	2026-06-30	8.8	CVE-2026-48307
advancedcoding--Comments wpDiscuz	The Comments - wpDiscuz plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the guest commenter 'Website' field in versions up to, and including, 7.6.56 This is due to insufficient output escaping in the getCommentAuthor() function, which interpolates the stored comment_author_url value directly into single-quoted HTML attributes without applying esc_url() or esc_attr(). This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-03	7.2	CVE-2026-9148
Advantech--Hospital Queuing Management	Hospital Queuing Management developed by Advantech has a Sensitive Data Exposure vulnerability, allowing unauthenticated remote attackers to access a specific URL to obtain API documentation.	2026-06-30	9.8	CVE-2026-14162
Advantech--Hospital Queuing Management	Hospital Queuing Management developed by Advantech has a Sensitive Data Exposure vulnerability, allowing unauthenticated remote attackers to access a specific URL to obtain API documentation.	2026-06-30	7.5	CVE-2026-14161
Ahmadgb--GeekyBot	Unauthenticated SQL Injection in GeekyBot <= 1.2.5 versions.	2026-07-02	9.3	CVE-2026-57679
ajith-ab--react-native-receive-sharing-intent	react-native-receive-sharing-intent contains a path traversal vulnerability that allows a co-resident malicious application to write files outside the intended cache directory by supplying a crafted _display_name value containing dot-dot path components through a malicious ContentProvider. Attackers can fire an explicit ACTION_SEND intent at the consuming app's exported share-receiver activity to overwrite arbitrary files in the consuming app's private data directory, including databases, shared preferences, and cached configuration, with attacker-controlled content.	2026-07-02	7.7	CVE-2026-58460
AncoraThemes--Lighthouse	Unauthenticated Local File Inclusion in Lighthouse <= 1.2.12 versions.	2026-07-02	8.1	CVE-2025-58902
Andy Fragen--WP Debugging	Unauthenticated Cross Site Scripting (XSS) in WP Debugging <= 2.12.2 versions.	2026-07-02	7.1	CVE-2026-57350
Anyscale, Inc--Ray	Ray prior to 2.56.0 contains an unsafe deserialization vulnerability in the WebDataset reader that allows attackers to achieve remote code execution by supplying a malicious tar archive to the read_webdataset() function. The _default_decoder() function in webdataset_datasource.py unconditionally calls pickle.loads() on tar entries with .pkl/.pickle extensions and torch.load() with weights_only=False on .pt/.pth entries, executing arbitrary code inside Ray remote workers on every worker that processes the malicious archive.	2026-07-01	8.8	CVE-2026-57516
apereo--cas	Apereo CAS 7.3.0 before 8.0.0-RC6 contains a cryptographic vulnerability that allows remote unauthenticated attackers to recover plaintext conversation state by exploiting AES-GCM initialization vector reuse across the server lifetime. Attackers can collect multiple client-side webflow execution tokens from the unauthenticated login page and perform known-plaintext analysis to decrypt the webflow conversation state due to	2026-07-02	9.1	CVE-2026-59099

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	keystream reuse caused by a fixed all-zero IV paired with the same encryption key.			
Arraytics--Booktics	Unauthenticated PHP Object Injection in Booktics <= 1.0.21 versions.	2026-07-02	9.8	CVE-2026-57621
Arraytics--Timetics	Unauthenticated Cross Site Scripting (XSS) in Timetics <= 1.0.58 versions.	2026-07-02	7.1	CVE-2026-57674
ASE--Admin and Site Enhancements (ASE) Pro	Unauthenticated Cross Site Scripting (XSS) in Admin and Site Enhancements (ASE) Pro <= 8.8.5 versions.	2026-07-02	9.6	CVE-2026-57625
Astoundify--Jobify	Unauthenticated Cross Site Scripting (XSS) in Jobify <= 4.3.2 versions.	2026-06-29	7.1	CVE-2026-57336
attr project--attr	attr before version 2.6.0 contains a symlink traversal vulnerability in the getfattr and setfattr utilities that allows local attackers to escalate privileges by replacing a pathname component with a symbolic link during directory hierarchy traversal. Attackers who control a pathname component can redirect getfattr and setfattr operations to arbitrary files by substituting a symlink, leading to local privilege escalation when getfattr or setfattr is invoked by a privileged process over an attacker-controlled path.	2026-06-29	7.1	CVE-2026-54371
AWS--Amazon CloudFront	Inconsistent interpretation of HTTP/2 requests in Amazon CloudFront with AWS WAF enabled might allow remote actors to bypass AWS WAF managed rule body inspection via crafted HTTP/2 requests that fragment the request body across frames so that only a partial body is inspected. This issue was remediated server-side. No customer action is required.	2026-06-29	9.8	CVE-2026-13762
AWS--AWS Advanced JDBC Wrapper	Deserialization of untrusted data in the RemoteQueryCachePlugin in Amazon Web Services AWS Advanced JDBC Wrapper 3.3.0 through 4.0.0 might allow an actor with write access to the shared cache infrastructure to execute arbitrary code on application servers that read cached query results via a crafted serialized Java object. The RemoteQueryCachePlugin uses ObjectInputStream without class filtering when deserializing cached query results from Redis or Valkey, enabling gadget chain execution when cache entries are poisoned. We recommend upgrading to AWS Advanced JDBC Wrapper version 4.0.1 or later.	2026-07-01	7.5	CVE-2026-14265
AWS--AWS Application Load Balancer	Inconsistent interpretation of HTTP/2 requests in AWS Application Load Balancer with AWS WAF enabled might allow remote actors to bypass AWS WAF managed rule body inspection via crafted HTTP/2 requests that fragment the request body across frames so that only a partial body is inspected. This issue only impacts HTTP/2 ALB target groups. To remediate this issue, customers should enable the "Inspect after sufficient data" target group configuration associated to an ALB load balancer. Refer to: (https://docs.aws.amazon.com/elasticloadbalancing/latest/application/edit-target-group-attributes.html#waf-http2-inspection)	2026-06-29	9.8	CVE-2026-13763
AWS--AWS CDK	OS command injection in the NodejsFunction Docker bundling pipeline (OsCommand helper) in AWS aws-cdk-lib on all platforms might allow a actor who controls dependency version strings in a project's package.json file to execute arbitrary commands on the host running the CDK toolchain via injected shell metacharacters in the OsCommand helper. This issue requires the actor to control the content of a package.json dependency version string that is processed during Docker-based bundling with nodeModules specified. To remediate this issue, users should upgrade to v2.260.0.	2026-07-01	7.3	CVE-2026-13760
Ays Pro--Survey Maker	Unauthenticated Cross Site Scripting (XSS) in Survey Maker <= 5.2.2.5 versions.	2026-07-02	7.1	CVE-2026-57361
BeRocket--Permalink Manager for WooCommerce	Unauthenticated Cross Site Request Forgery (CSRF) in Permalink Manager for WooCommerce <= 1.0.8.2 versions.	2026-07-02	7.1	CVE-2026-57758

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
BlueAstralTheme--SEOWP	Unauthenticated Cross Site Request Forgery (CSRF) in SEOWP <= 3.12.2 versions.	2026-07-02	7.1	CVE-2026-57761
BMC--Control-M/Enterprise Manager	Messaging consumer functionality allows deserialization of user-controlled data without sufficient restriction of allowed object types in the out of support Control-M/Server and Control-M/Enterprise Manager versions 9.0.20.x and potentially earlier. This issue may allow an authenticated attacker to trigger unintended server-side behavior through crafted serialized content.	2026-07-01	8	CVE-2026-10538
BMC--Control-M/Server	A Control-M/Server communication command does not sufficiently filter or sanitize user-supplied input. Under certain conditions, this issue may allow an unauthenticated attacker to execute unauthorized commands on the affected server, potentially leading to compromise of the server. This vulnerability affects Control-M/Server versions 9.0.20.x to 9.0.21.200 (included) and potentially earlier unsupported versions.	2026-07-01	9	CVE-2026-10539
BoldGrid--W3 Total Cache	Unauthenticated Arbitrary Code Execution in W3 Total Cache <= 2.9.4 versions.	2026-07-02	9	CVE-2026-57623
Capgo--Capgo	Capgo before 12.128.2 contains a broken object level authorization vulnerability in middlewareKey() that accepts the client-controlled x-limited-key-id header without validating ownership, allowing authenticated users to adopt cross-tenant limited keys. Attackers can supply another tenant's limited key ID to bypass authorization checks and access unauthorized cross-tenant resources across multiple API endpoints.	2026-06-30	8.8	CVE-2026-56230
Capgo--Capgo	Capgo before 12.128.2 contains a path traversal vulnerability in the builder upload proxy that allows authenticated users with build permissions to bypass upload restrictions. Attackers can append traversal sequences to the upload path, which are normalized by the WHATWG URL parser, enabling access to internal administrative endpoints with the privileged BUILDER_API_KEY header and resulting in server-side privilege escalation.	2026-06-30	8.3	CVE-2026-56233
Capgo--Capgo	Capgo before 12.128.2 allows org admins to assign org-scoped RBAC roles at app scope without validating role scope compatibility, including to pending invitees. Attackers can pre-seed malformed high-privilege bindings that survive invite acceptance, enabling accepted low-privilege users to perform unauthorized privileged app actions.	2026-06-30	8.8	CVE-2026-56247
Capgo--Capgo	Capgo before 12.128.2 contains an authentication bypass vulnerability in the account deletion endpoint that allows deletion without password re-authentication or secondary verification. Attackers can delete user accounts via session hijacking, CSRF attacks, or parameter tampering, resulting in unauthorized account deletion, data loss, and denial-of-service.	2026-06-30	8.1	CVE-2026-56286
Capgo--Capgo	Capgo before 12.128.2 contains a NULL-auth bypass vulnerability in the public.get_org_user_access_rbac function that allows unauthenticated attackers to retrieve RBAC role bindings and member email addresses. Attackers can exploit improper NULL comparison in the authorization gate to disclose organization membership, roles, and email addresses via the PostgREST RPC endpoint using only a public API key.	2026-06-30	7.5	CVE-2026-56219
Capgo--Capgo	Capgo before 12.128.2 contains an authorization bypass vulnerability in the channel creation endpoint that allows authenticated users to overwrite existing channels by reusing their names. Attackers with app.create_channel permission can exploit a logic mismatch between existence validation and upsert operations to reassign channel ownership and modify critical production channel configurations.	2026-06-30	7.6	CVE-2026-56249
Capgo--Capgo	Capgo before 12.128.2 contains unauthenticated security definer RPC functions get_user_id and get_org_perm_for_apikey that expose API key validity oracles and user UUID disclosure. Unauthenticated attackers using the public API key can validate leaked keys, enumerate users and apps, and determine permission levels, significantly increasing the actionability of compromised credentials.	2026-06-30	7.5	CVE-2026-56300
Capgo--Capgo	Capgo before 12.128.2 contains an authorization flaw in POST /private/create_device that accepts a caller-supplied org_id parameter	2026-06-30	7.1	CVE-2026-56320

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	without validating it matches the target app's owner organization. Authenticated attackers can create device records for an application using a foreign organization identifier, bypassing the intended org/app authorization boundary.			
ChaN--FatFs	In FatFs R0.16 and earlier contains a FAT32 integer overflow bug in mount_volume() where fsize *= fs->n_fats can wrap, leading to attacker-controlled file-size metadata and unsafe read lengths in downstream callers. This maps to CWE-190 (Integer Overflow or Wraparound). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (7.6, High). Remote delivery is also possible in OTA/update pipelines. The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Total.	2026-07-01	7.6	CVE-2026-6682
ChaN--FatFs	FatFs R0.16 and earlier contains a stack overflow bug in f_getlabel() because exFAT label length (XDIR_NumLabel) is trusted without enforcing spec maximums. This maps to CWE-121 (Stack-based Buffer Overflow). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (7.6, High). The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Total.	2026-07-01	7.6	CVE-2026-6687
ChaN--FatFs	FatFs R0.16 and earlier contains a downstream-caller vulnerability pattern associated with FatFs long filename handling. With LFN enabled, fno.fname can be up to 255 characters; many callers copy it into short fixed buffers without bounds checks, causing overflow. This maps to CWE-120 (Buffer Copy without Checking Size of Input). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H (7.6, High). The estimated CISA SSVC vectors are Exploitation: PoC, Technical Impact: Total.	2026-07-01	7.6	CVE-2026-6688
Chill Media Labs S.R.L.--Modula - PRO	Unauthenticated Cross Site Scripting (XSS) in Modula - PRO <= 2.10.8 versions.	2026-07-02	7.1	CVE-2026-57426
Cisco--Cisco Catalyst Center	A vulnerability in Cisco Catalyst Center could allow an unauthenticated, remote attacker to read arbitrary files from a restricted container. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to read arbitrary files from a restricted container of the affected device.	2026-07-01	7.5	CVE-2026-20191
Cisco--Cisco Secure Endpoint	A vulnerability in the PE file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in PE files during scanning, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted file that contains PE content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	2026-07-01	7.5	CVE-2026-20213
Cisco--Cisco Secure Endpoint	A vulnerability in the FSG file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in FSG files during scanning, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted file that contains portable executable content compressed with FSG to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	2026-07-01	7.5	CVE-2026-20214
Cisco--Cisco Secure Endpoint	A vulnerability in the 7z file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in 7z files during scanning, which may result in an out-of-bounds buffer	2026-07-01	7.5	CVE-2026-20215

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	write. An attacker could exploit this vulnerability by submitting a crafted file that contains 7z content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.			
Cisco--Cisco Secure Endpoint	A vulnerability in the InstallShield file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to improper handling of temporary resources during file scanning. An attacker could exploit this vulnerability by submitting a crafted InstallShield file to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to terminate the ClamAV scanning process and temporarily consume available system resources, resulting in a DoS condition on the affected software.	2026-07-01	7.5	CVE-2026-20216
Cisco--Cisco Secure Endpoint	A vulnerability in the PESpin file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in PESpin files during scanning, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted file that contains PESpin content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	2026-07-01	7.5	CVE-2026-20217
Cisco--Cisco Secure Endpoint	A vulnerability in the ALZ file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in ALZ files during scanning, which may result in an out-of-bounds buffer write. An attacker could exploit this vulnerability by submitting a crafted file that contains ALZ content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	2026-07-01	7.5	CVE-2026-20243
Cisco--Cisco Secure Endpoint	A vulnerability in the DMG file format parser of ClamAV could allow an unauthenticated, remote attacker to cause a DoS condition, or possibly other expanded impacts, resulting from memory corruption on an affected device. This vulnerability is due to improper boundary checks for content in DMG files during scanning, which may result in an integer overflow on 32-bit platforms only. An attacker could exploit this vulnerability by submitting a crafted file that contains DMG content to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to terminate, resulting in a DoS condition on the affected software.	2026-07-01	7.5	CVE-2026-20244
cmsjunkie--WP-BusinessDirectory plugin for WordPress	The WP-BusinessDirectory plugin for WordPress is vulnerable to Unauthenticated Arbitrary File Deletion in versions up to and including 4.0.1. This is due to insufficient path validation in the remove() method of the JBusinessDirectoryControllerUpload class. The task=upload.remove endpoint is accessible without authentication via the plugin's frontend routing system. The _filename parameter is accepted with RAW filter (no sanitization), and the helper function makePathFile() only normalizes directory separator characters without stripping path traversal sequences (../). When combined with the _path_type=2 parameter, which sets the base directory to the plugin's site folder, an attacker can supply a _filename value containing ../ sequences to traverse outside the plugin directory and call PHP's unlink() on arbitrary files - including wp-config.php, wp-config-backup.php, or other critical server files accessible to the web server process. This makes it possible for unauthenticated attackers to delete arbitrary files on the server.	2026-07-01	9.1	CVE-2026-6070

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cockpit-project--cockpit	Cockpit CMS before release 364 contains a path traversal and local file inclusion vulnerability that allows unauthenticated attackers to read arbitrary files or execute PHP files by including unvalidated PATH_INFO derived from REQUEST_URI in filesystem path construction without containment checks. Attackers can inject dot-dot sequences into the URL to traverse outside the designated spaces directory, and when the resolved path ends with a .php extension, the application passes it to include(), enabling local file inclusion on deployments using the PHP built-in server or certain non-default Nginx configurations.	2026-07-02	7.5	CVE-2026-58467
code-projects--Hotel and Tourism Reservation	A flaw has been found in code-projects Hotel and Tourism Reservation 1.0. Affected is an unknown function of the file /admin/add_room.php. Executing a manipulation of the argument delete_image/edit/description/number/price/rooms/type can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used.	2026-07-05	7.3	CVE-2026-14754
code-projects--Hotel and Tourism Reservation	A vulnerability has been found in code-projects Hotel and Tourism Reservation 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/reservations.php of the component Reservations Management Page. The manipulation of the argument delete leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2026-07-05	7.3	CVE-2026-14755
code-projects--Hotel and Tourism Reservation	A vulnerability was found in code-projects Hotel and Tourism Reservation 1.0. Affected by this issue is some unknown functionality of the file /admin/add_tour.php of the component Tour Management Page. The manipulation of the argument delete_image results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	2026-07-05	7.3	CVE-2026-14756
code-projects--Hotel and Tourism Reservation	A vulnerability was detected in code-projects Hotel and Tourism Reservation 1.0. The impacted element is an unknown function of the file /admin/rooms.php of the component Room Management Page. The manipulation of the argument delete results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	2026-07-05	7.3	CVE-2026-14762
code-projects--Hotel and Tourism Reservation	A flaw has been found in code-projects Hotel and Tourism Reservation 1.0. This affects an unknown function of the file /admin/tour_reserves.php of the component Tour Reservations Page. This manipulation of the argument tour causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	2026-07-05	7.3	CVE-2026-14763
code-projects--Hotel and Tourism Reservation	A vulnerability has been found in code-projects Hotel and Tourism Reservation 1.0. This impacts an unknown function of the file /admin/add_event.php of the component Event Management Page. Such manipulation of the argument fdetails leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2026-07-05	7.3	CVE-2026-14764
code-projects--Internship Management System	A security vulnerability has been detected in code-projects Internship Management System 1.0. The impacted element is an unknown function of the file employer/login.php of the component Employer Login Endpoint. The manipulation of the argument email/password leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	2026-07-05	7.3	CVE-2026-14700
code-projects--Online Examination	A vulnerability was determined in code-projects Online Examination 1.0. Affected by this issue is some unknown functionality of the file head.php. Executing a manipulation of the argument uname/password can lead to sql injection. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized.	2026-07-05	7.3	CVE-2026-14705
code-projects--Online Job Portal	A vulnerability was found in code-projects Online Job Portal 1.0. The affected element is an unknown function of the file login.php. Performing a manipulation of the argument txtUser/txtPass results in sql injection. The attack may be initiated remotely. The exploit has been made public and could be used.	2026-07-04	7.3	CVE-2026-14660

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects--Online Voting System	A security vulnerability has been detected in code-projects Online Voting System up to 0.x/1.0. This issue affects the function test_input of the file /authentication.php of the component Login. Such manipulation of the argument adminUserName/adminPassword leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used.	2026-07-04	7.3	CVE-2026-14648
code-projects--Online Voting System	A vulnerability was detected in code-projects Online Voting System 1.0. Impacted is the function test_input of the file /saveVote.php. Performing a manipulation of the argument voterName/voterEmail/voterID/selectedCandidate results in sql injection. The attack can be initiated remotely.	2026-07-04	7.3	CVE-2026-14649
code-projects--Real State Services	A weakness has been identified in code-projects Real State Services 1.0. Impacted is an unknown function of the file /single-list_sale.php?action=add. Executing a manipulation of the argument ID can lead to sql injection. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks.	2026-06-29	7.3	CVE-2026-13559
code-projects--Real State Services	A vulnerability was identified in code-projects Real State Services 1.0. The impacted element is an unknown function of the file /normalHomeSale.php. Such manipulation of the argument loc leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	2026-07-05	7.3	CVE-2026-14743
code-projects--Real State Services	A security flaw has been discovered in code-projects Real State Services 1.0. This affects an unknown function of the file /normalHomeRent.php. Performing a manipulation of the argument loc results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	2026-07-05	7.3	CVE-2026-14744
code-projects--Real State Services	A weakness has been identified in code-projects Real State Services 1.0. This impacts an unknown function of the file /single-list_rent.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks.	2026-07-05	7.3	CVE-2026-14745
code-projects--Real State Services	A security vulnerability has been detected in code-projects Real State Services 1.0. Affected is an unknown function of the file /addprojectrent.php. The manipulation of the argument amen leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	2026-07-05	7.3	CVE-2026-14746
code-projects--Real State Services	A vulnerability was detected in code-projects Real State Services 1.0. Affected by this vulnerability is an unknown functionality of the file /addprojectsale.php. The manipulation of the argument amen results in sql injection. The attack can be launched remotely.	2026-07-05	7.3	CVE-2026-14747
code-projects--Real State Services	A weakness has been identified in code-projects Real State Services 1.0. This vulnerability affects unknown code of the file /builderHome.php. This manipulation of the argument loc causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	2026-07-05	7.3	CVE-2026-14768
code-projects--Real State Services	A security vulnerability has been detected in code-projects Real State Services 1.0. This issue affects some unknown processing of the file /pay.php. Such manipulation of the argument Bankname leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	2026-07-05	7.3	CVE-2026-14769
code-projects--Smart Parking System	A vulnerability has been found in code-projects Smart Parking System 1.0. The affected element is an unknown function of the file /parkings/parkings.php. Such manipulation of the argument street/city/status leads to sql injection. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	2026-07-05	7.3	CVE-2026-14735
CodeAstro--Apartment Visitor	A vulnerability was found in CodeAstro Apartment Visitor Management System 1.0. Affected is an unknown function of the file /index.php of the component Login. Performing a manipulation of the argument Username	2026-07-04	7.3	CVE-2026-14640

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.			
Codepeople--Google Maps CP	Unauthenticated Cross Site Scripting (XSS) in Google Maps CP <= 1.2.5 versions.	2026-07-02	7.1	CVE-2026-57670
CoderPress--NOWPayments for WooCommerce	Unauthenticated Broken Access Control in NOWPayments for WooCommerce <= 1.4.0 versions.	2026-07-02	7.5	CVE-2026-39448
conductor-oss--conductor	Orkes Conductor 3.21.21 before 3.30.2 contains an unauthenticated remote code execution vulnerability that allows remote attackers to execute arbitrary OS commands by submitting inline workflow definitions containing malicious JavaScript or Python expressions to the workflow API endpoint prior to authentication. Attackers can exploit unsandboxed GraalVM evaluators configured with HostAccess.ALL or allowAllAccess(true) through INLINE, LAMBDA, DO_WHILE, and SWITCH task types to invoke arbitrary system commands via Java reflection or direct subprocess calls.	2026-06-30	9.8	CVE-2026-58138
Connekt Media--Ajax Load More - Filters	The Ajax Load More - Filters plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'taxonomy_include_children' parameter in all versions up to, and including, 3.4.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-30	7.2	CVE-2026-8141
Contempoinc--Real Estate 7	Unauthenticated Cross Site Scripting (XSS) in Real Estate 7 <= 3.5.9 versions.	2026-07-02	7.1	CVE-2026-57343
Control Web Panel--Control Web Panel	Control Web Panel before 0.9.8.1225 contains a blind SQL injection vulnerability that allows unauthenticated remote attackers to execute arbitrary SQL queries by submitting unsanitized input through the userRes POST parameter at the user endpoint. Attackers can exploit MySQL root privileges obtained via the injection to write arbitrary files using INTO DUMPFILE, enabling deployment of a PHP webshell to the web-accessible roundcube logs directory and achieving remote code execution as the cwpsvc account.	2026-07-01	9.8	CVE-2026-57517
coollabsio--coolify	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, Coolify's API controllers consistently validate server ownership with Server::whereTeamId(\$teamId) before any operation. However, multiple Livewire web UI components accept server_id and destination_uuid from URL query parameters without any team ownership validation, allowing cross-team resource deployment. This vulnerability is fixed in 4.0.0-beta.474.	2026-06-29	9.6	CVE-2026-57498
coollabsio--coolify	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.464, an authenticated command injection vulnerability in the CA Certificate management feature allows any authenticated user to execute arbitrary commands as the configured SSH user on the managed server host. As the SSH user typically would have to either be root or part of the docker group for Coolify to function as intended, this provides complete compromise of the managed server and associated docker containers. This vulnerability is fixed in 4.0.0-beta.464.	2026-06-30	8.8	CVE-2026-27957
coollabsio--coolify	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, an authenticated command injection vulnerability in the Destination Network Management functionality allows users with destination management permissions to execute arbitrary commands as root on managed servers. The "network" parameter is passed directly to shell commands without proper sanitization, enabling full remote code execution on the host system. This vulnerability is fixed in 4.0.0-beta.471.	2026-06-29	8.8	CVE-2026-34594

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
coolabsio--coolify	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.470, a critical Authenticated Host Remote Code Execution (RCE) vulnerability was discovered in Coolify. The flaw resides in the handling of user-defined build parameters for the Nixpacks build pack. Specifically, the install_command provided by a user is directly concatenated into a shell command string that is executed on the deployment host during the building phase. An attacker can leverage this to escape the intended build context and execute arbitrary commands with host-level privileges. This vulnerability is fixed in 4.0.0-beta.470.	2026-06-29	8.8	CVE-2026-34597
coolabsio--coolify	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.471, Coolify server and project lookups are not scoped to the current team, allowing any authenticated user to access servers and projects belonging to other teams by specifying their IDs directly. This vulnerability is fixed in 4.0.0-beta.471.	2026-06-29	7.7	CVE-2026-34592
coolabsio--coolify	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.474, the HMAC key is the application's manual_webhook_secret_github field, which is used by Coolify's webhook endpoints to validate incoming requests, is nullable with no default - meaning newly created applications have a null webhook secret. PHP's hash_hmac() function silently coerces a null key to an empty string ". So when the secret is null, the server computes hash_hmac('sha256', \$payload, '') - a deterministic value that any attacker can calculate independently. By sending X-Hub-Signature-256: sha256=<hash_hmac('sha256', payload, '')>, an unauthenticated attacker can forge a valid signature and trigger deployments. This vulnerability is fixed in 4.0.0-beta.474.	2026-06-29	7.5	CVE-2026-41896
Cozmoslabs--Paid Member Subscriptions	Unauthenticated Server Side Request Forgery (SSRF) in Paid Member Subscriptions <= 3.0.4 versions.	2026-07-02	7.2	CVE-2026-57348
cozyvision1--SMS Alert SMS & OTP for WooCommerce, Order Notifications & Abandoned Cart Recovery	The SMS Alert - SMS & OTP for WooCommerce, Order Notifications & Abandoned Cart Recovery plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 3.9.5. This is due to the plugin not properly validating a user's identity prior to updating their details like reset the password of any user account, including administrators, and gain full access to those accounts. This makes it possible for unauthenticated attackers to change arbitrary user's email addresses, including administrators, and leverage that to reset the user's password and gain access to their account. This is only vulnerable on sites with OTP verification for password resets enabled, and where the administrator (or other user) has set a phone number for OTP verification.	2026-07-01	9.8	CVE-2026-11387
Crawl4AI--Crawl4AI	Crawl4AI before 0.8.7 contains an arbitrary JavaScript execution vulnerability in the Docker API server's /execute_js endpoint, which accepts and executes arbitrary user-supplied JavaScript in the server's browser context with --disable-web-security enabled. An attacker can execute arbitrary JavaScript and, combined with the browser's relaxed security settings, perform server-side request forgery against internal services.	2026-06-30	8.1	CVE-2026-56264
Creative Themes--Blocksy Companion Pro	Unauthenticated Remote Code Execution (RCE) in Blocksy Companion Pro <= 2.1.46 versions.	2026-07-02	10	CVE-2026-57624
D-Link--DCS-935L	A vulnerability has been found in D-Link DCS-935L 1.10.01. This affects the function sub_400E40 of the file setconf.cgi of the component POST Parameter Handler. Such manipulation of the argument UID leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2026-06-29	8.8	CVE-2026-13545
dapr--dapr	Dapr Sentry's OIDC discovery endpoint derives the issuer and jwks_uri of the /.well-known/openid-configuration document from the request Host,	2026-07-02	7.5	CVE-2026-59096

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	honoring an attacker-controlled X-Forwarded-Host header without validation when no allowed-hosts list is configured (the default), and serves the document with a one-hour public cache lifetime. A remote unauthenticated attacker can poison the discovery document so relying parties performing dynamic (unpinned) discovery fetch the JWKS from an attacker-controlled server, causing attacker-signed JWTs to be accepted. Exploitation requires the OIDC server enabled without a configured jwt-issuer or oidc-allowed-hosts.			
Dassault Systmes--BIOVIA Workbook	A Race Condition vulnerability affecting BIOVIA Workbook from Release 2021 through Release 2026 could allow a user to access unauthorized data from another user.	2026-07-01	8.1	CVE-2026-5120
databasebackup--WP Database Backup Unlimited Database & Files Backup by Backup for WP	The WP Database Backup - Unlimited Database & Files Backup by Backup for WP plugin for WordPress is vulnerable to OS Command Injection in all versions up to and including 7.11 via the `wp_db_exclude_table` parameter. This is due to the direct concatenation of user-supplied `\$_POST['wp_db_exclude_table']` values into the `mysqldump` shell command string in the `mysqldump()` function of `includes/admin/class-wpdb-admin.php` without wrapping them in `escapeshellarg()`-every other argument in the same command (DB_USER, DB_PASSWORD, host, filename, DB_NAME) is properly escaped, making the exclude-table values the sole exception-and because the only applied filtering, `sanitize_text_field()` via `recursive_sanitize_text_field()`, strips HTML tags but leaves shell metacharacters such as `;`, ` `, `` ` ``, and `\$()` intact. This makes it possible for authenticated attackers, with administrator-level access and above, to execute arbitrary operating system commands on the server, potentially enabling full remote code execution. The injection is stored: malicious values submitted through the plugin settings form are persisted to the WordPress options table via `update_option('wp_db_exclude_table')` and later retrieved with `get_option()` and passed unsanitized to `shell_exec()` whenever a backup operation runs.	2026-07-02	7.2	CVE-2026-9834
Dell--Device Management Agent	Dell Device Management Agent, versions prior to DDMA 26.05, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	2026-07-01	7.3	CVE-2026-41121
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution.	2026-07-03	7.2	CVE-2026-49814
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper neutralization of special Elements used in an OS command ('OS command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to execution of arbitrary OS commands.	2026-07-03	7.2	CVE-2026-49815
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper neutralization of special elements used in an OS command ('OS command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to command execution.	2026-07-03	7.2	CVE-2026-53478
deltaww--AS228T	AS228T with Authentication Bypass Vulnerability	2026-07-01	7.4	CVE-2026-12579

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
deltaww--DVP80ES3	DVP80ES3 with Improper Resource Shutdown or Release vulnerability.	2026-07-01	7.5	CVE-2026-12575
deltaww--DVP80ES3	DVP80ES3 with Improper Enforcement of Message Integrity During Transmission in a Communication Channel vulnerability.	2026-07-01	7.5	CVE-2026-12576
deltaww--DVP80ES300T	DVP80ES300T with Improper Validation of Array Index Vulnerability	2026-07-01	7.5	CVE-2026-14193
Design themes--Kids Zone - Children WordPress Theme	Unauthenticated Cross Site Scripting (XSS) in Kids Zone - Children WordPress Theme <= 5.4 versions.	2026-07-02	7.1	CVE-2025-69156
Designthemes--Fitness Zone WordPress Theme	Unauthenticated Cross Site Scripting (XSS) in Fitness Zone WordPress Theme <= 5.7 versions.	2026-07-02	7.1	CVE-2025-69155
Designthemes--Kids Life Children School WordPress	Unauthenticated Cross Site Scripting (XSS) in Kids Life Children School WordPress <= 5.2 versions.	2026-07-02	7.1	CVE-2026-27402
Designthemes--LMS	Unauthenticated Cross Site Scripting (XSS) in LMS <= 9.7 versions.	2026-07-02	7.1	CVE-2026-27404
designthemes--SpaLab Beauty Salon WordPress Theme	Unauthenticated Cross Site Scripting (XSS) in SpaLab Beauty Salon WordPress Theme <= 6.7 versions.	2026-07-02	7.1	CVE-2025-69154
designthemes--Trendy Travel	Unauthenticated Cross Site Scripting (XSS) in Trendy Travel <= 6.7 versions.	2026-07-02	7.1	CVE-2025-69153
dhruvin--Custom Payment Gateways for WooCommerce	The Custom Payment Gateways for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'alg_wc_cpg_input_fields' parameter in all versions up to, and including, 2.1.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This vulnerability is exploitable by unauthenticated guest users submitting a crafted checkout POST request, requiring no custom input fields to be configured in the plugin.	2026-07-01	7.2	CVE-2026-7517
Divi Engine--Divi Form Builder	The Divi Form Builder plugin for WordPress is vulnerable to Arbitrary File Upload leading to Remote Code Execution in all versions up to and including 5.1.8. This is due to insufficient file extension validation in the do_image_upload() function where user-supplied input from the acceptFileTypes POST parameter is directly interpolated into a regular expression used to validate uploaded files. Attackers can specify PHP-executable extensions such as .phtml, .phar, .php5, or .php7 to bypass the plugin's .htaccess protection which only blocks .php files specifically. Additionally, on Nginx-based servers, the .htaccess protection is completely ineffective as Nginx does not process .htaccess files. This makes it possible for unauthenticated attackers (who can obtain a nonce from any public page containing a form) to upload executable PHP files to the publicly accessible /wp-content/uploads/de_fb_uploads/ directory and achieve Remote Code Execution by accessing the uploaded file via HTTP. The vulnerability was partially patched in version 5.1.3.	2026-07-02	9.8	CVE-2026-5524
Dolibarr--dolibarr	Dolibarr through 23.0.3, fixed in commit 14db36e, contains a sql injection vulnerability that allows authenticated API users to exfiltrate arbitrary database contents by supplying malicious values to the sqlfilters query parameter in the setup dictionary and multicurrencies REST API endpoints. The affected endpoints in api_setup.class.php and api_multicurrencies.class.php validate sqlfilters only for balanced parentheses and rewrite matched triplets, allowing text placed outside the expected shape such as an appended UNION SELECT to be concatenated	2026-06-30	7.6	CVE-2026-58376

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	into the SQL WHERE clause unmodified, enabling retrieval of sensitive data including password hashes and API keys.			
e4jvikwp--VikBooking Hotel Booking Engine & PMS	Cross-Site Request Forgery (CSRF) vulnerability in e4jvikwp VikBooking Hotel Booking Engine & PMS allows Path Traversal. This issue affects VikBooking Hotel Booking Engine & PMS: from n/a through 1.8.12.	2026-07-01	7.4	CVE-2026-57723
Eclipse Foundation--Eclipse CSI - PIA	PIA's OIDC issuer allowlist for Jenkins tokens uses a bare string-prefix check (issuer.startswith(' https://ci.eclipse.org ') in is_issuer_known, pia/models.py:139) instead of validating the issuer as a properly host-bounded URL. An attacker can craft an issuer such as https://ci.eclipse.org@evil.host (userinfo trick) or https://ci.eclipse.org.evil.host (suffix trick) that satisfies the prefix check while pointing the OIDC discovery and JWKS fetches at a server the attacker controls. An unauthenticated caller of POST /v1/upload/sbom can use this to force PIA to make outbound HTTP(S) requests to an arbitrary attacker-chosen host, and to have oidc.verify_token accept a JWT signed with the attacker's own key.	2026-07-02	8.2	CVE-2026-14336
Eclipse Foundation--Eclipse Parsson	In Eclipse Parsson published Maven Central artifacts before version 1.1.8, the JSON parser did not enforce a default maximum on the number of characters consumed while parsing a single JSON document. Applications that parse attacker- controlled JSON can be forced to consume excessive CPU and memory by processing very large documents, including large arrays, objects, strings, numbers, whitespace, or nested structures, resulting in a denial of service. Eclipse Parsson 1.1.8 introduces a configurable maximum parsing limit with a default limit of 15 million parser-consumed characters.	2026-07-02	7.5	CVE-2026-9563
Eclipse Foundation--Eclipse Theia	In affected versions of Eclipse Theia (1.8.1 and later), the browser backend exposes privileged terminal RPC over WebSocket (/services/shell-terminal, /services/terminals/:id) without service-level authentication. WebSocket origin validation in @theia/core is fail-open: connections are accepted when the Origin header is missing or when no THEIA_HOSTS allowlist is configured (the default). The Socket.IO integration additionally replaces the real Origin header with a client-supplied fix-origin header that an attacker can control or omit. As a result, a foreign-origin web page visited by a user with a running Theia instance can open the /services WebSocket namespace, invoke terminal creation, attach to the resulting terminal data channel, execute arbitrary OS commands, and read their output. This affects both local developer setups (drive-by attack) and hosted or tunneled deployments without strong external authentication. A fix is in development that enforces same-origin validation by default, removes trust in the fix-origin header, gates HTTP and WebSocket access on a SameSite=Strict; HttpOnly connection-token cookie, and sanitizes shell terminal creation options.	2026-07-03	8.8	CVE-2026-10054
Eclipse Foundation--Eclipse Theia	In Eclipse Theia since version 1.26.0, the backend /services/request-service RPC accepts an attacker-controlled URL from any client connected to the standard /services messaging endpoint, performs the HTTP request server-side, and returns the full response body to the caller. Because the destination URL is neither validated nor allowlisted, a remote attacker with access to the Theia service connection can issue server-side HTTP requests to localhost or other backend-reachable hosts and read their responses, exposing internal administrative endpoints, cloud instance metadata services, and other resources that are intentionally outside the browser network boundary. The vulnerability affects deployments where the Theia service connection is reachable by untrusted users (for example, multi-tenant or publicly-reachable Theia deployments).	2026-07-03	8.5	CVE-2026-10055
eclipse-wakaama--wakaama	Eclipse Wakaama before snapshot/2026-05-26 contains an unbounded memory allocation vulnerability in the CoAP Block1 handler within coap/block.c that allows unauthenticated remote attackers to exhaust server memory by sending a sequence of Block1 PUT requests with	2026-07-02	7.5	CVE-2026-58465

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	incrementing block numbers. Attackers can target the registration endpoint over UDP without authentication, causing the server to repeatedly reallocate a growing accumulation buffer by appending each block payload without enforcing any maximum total size limit, resulting in denial of service through memory exhaustion.			
Edimax--EW-7478APC	A flaw has been found in Edimax EW-7478APC 1.04. This affects the function formiNICSiteSurvey of the file /goform/formiNICSiteSurvey of the component POST Request Handler. This manipulation of the argument seSSID causes buffer overflow. It is possible to initiate the attack remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-29	8.8	CVE-2026-13562
Edimax--EW-7478APC	A vulnerability has been found in Edimax EW-7478APC 1.04. This impacts the function formL2TPSetup of the file /goform/formL2TPSetup of the component POST Request Handler. Such manipulation of the argument L2TPUserName leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-29	8.8	CVE-2026-13563
Edimax--EW-7478APC	A vulnerability was found in Edimax EW-7478APC 1.04. Affected is the function formPPPoESetup of the file /goform/formPPPoESetup of the component POST Request Handler. Performing a manipulation of the argument pppUserName results in stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-29	8.8	CVE-2026-13564
Edimax--EW-7478APC	A security vulnerability has been detected in Edimax EW-7478APC 1.04. This affects the function formQoS of the file /goform/formQoS of the component POST Request Handler. The manipulation of the argument seSSID leads to buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-29	8.8	CVE-2026-13580
Edimax--EW-7478APC	A flaw has been found in Edimax EW-7478APC 1.04. This issue affects the function formUSBAccount of the file /goform/formUSBAccount of the component POST Request Handler. This manipulation of the argument UserName/Password causes buffer overflow. The attack is possible to be carried out remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-29	8.8	CVE-2026-13582
Edimax--EW-7478APC	A vulnerability has been found in Edimax EW-7478APC 1.04. Impacted is the function formUSBFolder of the file /goform/formUSBFolder of the component POST Request Handler. Such manipulation of the argument ShareName/SelectName leads to buffer overflow. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-29	8.8	CVE-2026-13583
Eksagate Electronic Engineering and Computer Industry Trade Inc.--SYSGUARD 6001	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Eksagate Electronic Engineering and Computer Industry Trade Inc. SYSGUARD 6001 allows Blind SQL Injection. This issue affects SYSGUARD 6001: from 2.0.2 before 6.1.16.0. NOTE: The vendor was contacted and it was learned that the product is not supported.	2026-06-30	9.8	CVE-2026-8402
Elastic--Kibana	Improper Output Neutralization for Logs (CWE-117) in Kibana can lead to log injection via Log Injection-Tampering-Forging (CAPEC-93). An attacker can supply specially crafted input that is written to log files without proper neutralization. When the log files are subsequently viewed in a terminal that interprets control sequences, the injected content may alter the displayed log data.	2026-07-01	8	CVE-2026-49091

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Elated-Themes--Audrey	Unauthenticated Local File Inclusion in Audrey <= 1.5 versions.	2026-07-02	8.1	CVE-2026-42382
electron-userland--electron-builder	electron-updater allows for automatic updates for Electron apps. Prior to 26.15.0, AppImage targets built by app-builder-lib could use an empty path component when setting the LD_LIBRARY_PATH environment variable at runtime. This causes the current working directory to be added to the dynamic linker search path, which may allow an attacker to execute arbitrary code by placing a malicious shared library in the directory from which the AppImage is launched. This issue has been fixed in version 26.15.0.	2026-06-30	7.8	CVE-2026-54672
elemntor--Image Optimizer Optimize Images and Convert to WebP or AVIF	The Image Optimizer plugin for WordPress is vulnerable to arbitrary file deletion in versions up to and including 1.7.4. This is due to insufficient path validation in the Image_Backup::remove() function where backup file paths stored in post meta are used directly in file deletion operations without verifying they are within the uploads directory. The plugin stores backup file paths in the image_optimizer_metadata post meta field and trusts these paths completely when deleting backups on the delete_attachment hook. An authenticated attacker with Author-level access can edit the image_optimizer_metadata post meta on their own attachments via WordPress's Custom Fields interface, injecting arbitrary absolute file paths into the backups array. When the attacker subsequently deletes the attachment, the plugin calls File_System::delete() on each path without validation. This makes it possible for authenticated attackers, with Author-level access and above, to delete arbitrary files on the server within the web server's filesystem permissions, potentially leading to denial of service, data loss, or security degradation.	2026-07-02	8.1	CVE-2026-5821
emarket-design--Request a Quote Quote Forms for Any WordPress Site	The Request a Quote plugin for WordPress is vulnerable to Code Injection in versions up to, and including, 2.5.5 via the emd_delete_file AJAX action. This is due to the emd_delete_file() handler deriving a PHP function name from the attacker-controlled \$_POST['path'] parameter and invoking it dynamically via the variable-function call \$sess_name(), and the handler being registered for wp_ajax_nopriv with its only protection being a nonce that the plugin prints into the public quote-form page via wp_localize_script. This makes it possible for unauthenticated attackers to invoke arbitrary zero-argument PHP functions on the server, such as phpinfo(), potentially exposing sensitive server configuration and credentials, or executing other destructive built-in PHP functions.	2026-07-02	7.5	CVE-2026-14249
emarket-design--Video Gallery YouTube Gallery, Playlist & Video Grid	The Youtube Showcase plugin for WordPress is vulnerable to Arbitrary Function Call in versions up to and including 4.0.3. This is due to insufficient validation of the 'path' parameter in the emd_delete_file() AJAX handler in includes/common-functions.php. The user-supplied value is passed through sanitize_text_field(), has its trailing '_PLUGIN_DIR' substring stripped, and is then invoked as a PHP function name with no arguments via '\$sess_name()'. The handler is gated only by a nonce - no current_user_can() check is present - and the nonce is emitted on any front-end page that renders a form shortcode containing file fields. This makes it possible for authenticated attackers, with Subscriber-level access and above, to invoke arbitrary zero-argument PHP functions (such as phpinfo, phpversion, get_defined_vars, error_get_last), resulting in sensitive information disclosure and potential further compromise depending on the functions available in the environment.	2026-07-01	7.5	CVE-2026-12923
Empirum--Matrix42	PBackupVSS.exe in Matrix42 Empirum before 25.5 and 26.x before 26.2 creates a named pipe (\\.\pipe\PBackupVSS) with a DACL that grants GENERIC_READ and GENERIC_WRITE permissions to all authenticated users. A low-privileged local attacker can connect to this pipe and send crafted IPC messages to trigger execution of arbitrary commands with SYSTEM privileges via an untrusted search path. This allows privilege escalation by placing a malicious shadow.exe in a controlled working directory.	2026-06-29	7.8	CVE-2026-57919

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Epiphyt--Embed Privacy	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Epiphyt Embed Privacy allows Path Traversal. This issue affects Embed Privacy: from n/a through 1.12.3.	2026-06-29	7.1	CVE-2026-57346
Epsiloncool--WP Fast Total Search	Unauthenticated SQL Injection in WP Fast Total Search <= 1.80.280 versions.	2026-07-02	9.3	CVE-2026-57683
EstrellaXD--Auto_Bangumi	AutoBangumi before 3.2.8 contains a hard-coded default credentials vulnerability that allows unauthenticated attackers to authenticate as the administrator by using the publicly known default credentials seeded at startup via add_default_user() in the database user module when the users table is empty. Attackers can submit the default credentials to the authentication login endpoint to gain full control of the application, including RSS feed configuration, downloader configuration, and all authenticated API endpoints.	2026-07-02	9.8	CVE-2026-58466
etrue--WPeMatico RSS Feed Fetcher	Unauthenticated Cross Site Scripting (XSS) in WPeMatico RSS Feed Fetcher <= 2.8.17 versions.	2026-07-02	7.1	CVE-2026-57349
EventON--EventON (Pro) - WordPress Virtual Event Calendar Plugin	The EventON - WordPress Virtual Event Calendar Plugin plugin for WordPress (full) is vulnerable to SQL Injection via the WordPress 'search' parameter in versions up to, and including, 5.0.11 due to insufficient escaping on the user supplied parameter and lack of preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database, granted the "Enable additional search queries" setting is enabled and at least one published event exists.	2026-06-30	9.8	CVE-2026-9711
fast-uri--fast-uri	fast-uri versions 2.3.1 through 3.1.2 and 4.0.0 fail to canonicalize Unicode (IDN) hostnames for HTTP-family URLs. The IDN conversion path calls a helper that does not exist on the global URL constructor, silently leaving the host in its original Unicode form while normalize() and equal() still return values that differ from a WHATWG-compatible URL parser. Applications that use fast-uri to enforce host-based policy (denylists, loopback filtering, redirect validation, outbound proxy routing) before passing the same URL to Node's URL or fetch can be bypassed when the two implementations resolve the same input to different hosts. Patches: upgrade to fast-uri 3.1.3 for the 3.x line or 4.0.1 for the 4.x line. Workarounds: enforce host policy using the same URL parser used for the actual request, or reject non-ASCII hosts before policy checks.	2026-06-29	7.5	CVE-2026-13676
Feast--Feast Feature Server	A vulnerability has been identified in the Feast Feature Server's `/save-document` endpoint that allows an unauthenticated remote attacker to write arbitrary JSON files to the server's filesystem. Although the system attempts to restrict file locations, these protections can be bypassed, enabling an attacker to overwrite vital application configurations or startup scripts. Because this flaw requires no credentials or special privileges, any attacker with network access to the server can potentially compromise the integrity of the system. This could lead to unauthorized system modifications, denial of service through disk exhaustion, or potential remote code execution.	2026-07-01	9.1	CVE-2026-23537
Feehi--CMS	A vulnerability was found in Feehi CMS up to 2.1.1. This vulnerability affects unknown code of the file /api/articles of the component REST API Endpoint. Performing a manipulation results in missing authentication. The attack may be initiated remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-29	7.3	CVE-2026-13546
Flowise--Flowise	Flowise before 3.1.0 (affected versions 3.0.13 and earlier) uses a weak hardcoded default secret ('flowise') for the express-session middleware when the EXPRESS_SESSION_SECRET environment variable is not set (packages/server/src/enterprise/middleware/passport/index.ts). Because this default secret is publicly visible in the source code, an attacker can	2026-06-30	9.1	CVE-2026-56278

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	forge valid signed session cookies to impersonate any user and bypass authentication.			
Frangoteam--FUXA SCADA/HMI	FUXA versions 1.3.1 and prior contain an authentication bypass vulnerability via dot-segment path normalization in the REST API. The API router fails to normalize dot-segment sequences before applying authentication middleware, allowing unauthenticated requests to access protected endpoints by prefixing paths with dot-segments such as /api/./users, /api/./roles, and /api/project/./users. These requests bypass authentication checks and return sensitive user and role data without credentials.	2026-06-30	7.5	CVE-2026-13207
FrontAccounting--FrontAccounting	FrontAccounting before 2.4.20 contains a path traversal vulnerability in the attachment upload handler that allows authenticated attackers to execute arbitrary code by uploading files with traversal sequences in the unique_name parameter. Attackers can supply path traversal sequences ../../././shell.php to write files outside the intended attachments directory into the web root, and by uploading PHP files without extension validation, achieve remote code execution as the web server user.	2026-06-29	8.8	CVE-2026-40521
FrontAccounting--FrontAccounting	FrontAccounting before 2.4.20 contains a SQL injection vulnerability in the Audit Trail report handler that allows authenticated attackers with SA_GLANALYTIC permission to execute arbitrary SQL queries by injecting malicious code into the PARAM_2 and PARAM_3 POST parameters. Attackers can exploit time-based blind SQL injection through SLEEP() functions that are amplified across JOIN result sets to cause denial of service by exhausting database connections, or extract arbitrary database content through UNION-based injection techniques.	2026-06-29	8.1	CVE-2026-40523
FrontAccounting--FrontAccounting	FrontAccounting before 2.4.20 contains a SQL injection vulnerability in the get_gl_transactions() function where the filter_type parameter is concatenated directly into a SQL IN() clause without parameterization. Attackers with SA_GLANALYTIC permission can inject arbitrary SQL by supplying a closing parenthesis followed by malicious conditions to extract sensitive journal entry data through boolean-based blind SQL injection with reliable response size differentials.	2026-06-29	8.1	CVE-2026-40524
FrontAccounting--FrontAccounting	FrontAccounting before 2.4.20 contains a SQL injection vulnerability in the Bank Statement report handler that allows authenticated attackers to extract arbitrary database data by injecting UNION SELECT payloads into the PARAM_0 POST parameter. Attackers can supply malicious SQL syntax through the unparameterized WHERE clause to retrieve sensitive information including usernames, password hashes, and email addresses from the users table, rendered into PDF report output.	2026-06-29	7.1	CVE-2026-40522
Fuelthemes--Werkstatt	Contributor PHP Object Injection in Werkstatt <= 4.8.3 versions.	2026-07-02	8.8	CVE-2026-27414
Gardyn--Gardyn Home Firmware	Gardyn devices expose a privileged iotHubowner key. Access to this key will allow a malicious user to invoke an IoT Hub Registry Manager function which returns connection information for all Gardyn Home Kit and Studio devices. Access to this key also allows a malicious user to execute arbitrary commands on a specific connected device and may allow the malicious user to pivot to other devices on the user's network.	2026-07-02	10	CVE-2026-13768
GeoVision Inc.--GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. In order to access the websocket server, no authentication is required. As such, any malicious website can attempt to open a connection to the server and potentially access sensitive APIs. In particular, it's possible to call a combination of the `create` method and `getScreenCapture` to retrieve the content of the user's screen.	2026-07-02	8.8	CVE-2026-13125
GeoVision Inc.--GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with	2026-07-02	8.3	CVE-2026-13131

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. ##### connectInfo command index-out-of-bound			
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. ##### setStream command index-out-of-bound	2026-07-02	8.3	CVE-2026-13132
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. ##### setPIP command index-out-of-bound	2026-07-02	8.3	CVE-2026-57264
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. ##### audio command index-out-of-bound	2026-07-02	8.3	CVE-2026-57265
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. ##### 2wayAudio command index-out-of-bound	2026-07-02	8.3	CVE-2026-57266
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. ##### 2wayAudio command index-out-of-bound	2026-07-02	8.3	CVE-2026-57267

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. ##### snapshot command index-out-of-bound			
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. ### saveVideo command index-out-of-bound When sending the `saveVideo` command, the `index` field is extracted from the websocket message [1]. Then without checking the range of the index, it is used to trigger a CriticalSection ([2]) and releases it [3]. The release function call ([3]) is executed using a function pointer which will be read out of bounds potentially leading to code execution: v6 = get_entry(a2, "index"); result = json_is_value_int(v6); if ((_BYTE)result) { v8 = get_entry(a2, "index"); index = json_value_to_int(&v8->value); // [1] result = CCriticalSection::EnterCritSection(&this->crit_sections[index]); // [2] if (result) { if (this->array_of_IPCams[index]) { if (this->array_of_IPCams[index]->field_20) do_PostMessageA((CViewer *)this->array_of_IPCams[index], 0x111u, 0x139Fu, v11); } return (*(int (__thiscall **))(CCriticalSection *)) (this->crit_sections[index].vtbl + 20))(&this->crit_sections[index]); // [3] }	2026-07-02	8.3	CVE-2026-57268
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. ##### disconnect command index-out-of-bound	2026-07-02	8.3	CVE-2026-57269
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. ##### play command index-out-of-bound	2026-07-02	8.3	CVE-2026-57270
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. ##### pause command index-out-of-bound	2026-07-02	8.3	CVE-2026-57271
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with	2026-07-02	8.3	CVE-2026-57272

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. Many of the commands will take an `index` value that is then used to access various arrays to enter critical sections, perform various actions via function calls, etc. However the `index` value is usually not checked for valid range, and as such it can be used to access multiple arrays out-of-bound. ##### byPass command index-out-of-bound			
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. One of them, `connectionInfo` is meant to provide the necessary details to connect to a camera. The handler associated with this command that we call `handle_connection_info` contains multiple instances of string copy that can overflow. The function `handle_connect_info` copies attacker-controlled JSON strings into fixed-size buffers using manual byte-by-byte loops that do not enforce length limits. ##### Buffer Overflow in username field (no key present)	2026-07-02	8.3	CVE-2026-57273
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. One of them, `connectionInfo` is meant to provide the necessary details to connect to a camera. The handler associated with this command that we call `handle_connection_info` contains multiple instances of string copy that can overflow. The function `handle_connect_info` copies attacker-controlled JSON strings into fixed-size buffers using manual byte-by-byte loops that do not enforce length limits. ##### Buffer Overflow in password field (no key present)	2026-07-02	8.3	CVE-2026-57274
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. One of them, `connectionInfo` is meant to provide the necessary details to connect to a camera. The handler associated with this command that we call `handle_connection_info` contains multiple instances of string copy that can overflow. The function `handle_connect_info` copies attacker-controlled JSON strings into fixed-size buffers using manual byte-by-byte loops that do not enforce length limits. ##### Buffer Overflow in username field (key present)	2026-07-02	8.3	CVE-2026-57275
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. One of them, `connectionInfo` is meant to provide the necessary details to connect to a camera. The handler associated with this command that we call `handle_connection_info` contains multiple instances of string copy that can overflow. The function `handle_connect_info` copies attacker-controlled JSON strings into fixed-	2026-07-02	8.3	CVE-2026-57276

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	size buffers using manual byte-by-byte loops that do not enforce length limits. ##### Buffer Overflow in password field (key present)			
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. One of them, `connectionInfo` is meant to provide the necessary details to connect to a camera. The handler associated with this command that we call `handle_connection_info` contains multiple instances of string copy that can overflow. The function `handle_connect_info` copies attacker-controlled JSON strings into fixed-size buffers using manual byte-by-byte loops that do not enforce length limits. ##### Buffer Overflow in key field	2026-07-02	8.3	CVE-2026-57277
GeoVision Inc.-- GeoWebPlayer	GeoWebPlayer (also called "Web Plugin" in the GV-VMS documentation and "WS Player" for VMS-Cloud) is an addon that can be installed with various GeoVision software (GV-VMS, GV-Cloud, ...). It creates a websocket server that expands the capabilities of the various web-interfaces provided by the GeoVision software and may be necessary for them to function properly. The Websocket server can accept various commands coming from localhost. One of them, `connectionInfo` is meant to provide the necessary details to connect to a camera. The handler associated with this command that we call `handle_connection_info` contains multiple instances of string copy that can overflow. The function `handle_connect_info` copies attacker-controlled JSON strings into fixed-size buffers using manual byte-by-byte loops that do not enforce length limits. ##### Buffer Overflow in ip field	2026-07-02	8.3	CVE-2026-57278
Gitea--Gitea Open Source Git Server	Gitea Docker image versions up to and including 1.26.2 use REVERSE_PROXY_TRUSTED_PROXIES=* by default, allowing any source IP to impersonate a user when reverse-proxy authentication headers such as X-WEBAUTH-USER are enabled.	2026-07-03	9.8	CVE-2026-20896
Gitea--Gitea Open Source Git Server	Gitea versions up to and including 1.26.2 have incomplete SSRF protection in webhook and migration allow-list filtering.	2026-07-03	9.6	CVE-2026-22874
Gitea--Gitea Open Source Git Server	Gitea Actions Artifacts V4 signed URL HMAC ambiguity allows cross-repository artifact read and cross-task upload-state write	2026-07-03	9.6	CVE-2026-58426
Gitea--Gitea Open Source Git Server	Gitea versions before 1.26.0 allow API users to fork a repository into an organization without first passing the CanCreateOrgRepo check, which can expose organization secrets.	2026-07-03	8.1	CVE-2026-22555
Gitea--Gitea Open Source Git Server	Gitea versions up to and including 1.26.1 allow the Allow edits from maintainers permission path to authorize commits to repositories that the user can read but should not be able to write.	2026-07-03	8.5	CVE-2026-26231
Gitea--Gitea Open Source Git Server	Gitea versions up to and including 1.26.1 allow OAuth2 access token scope enforcement to be bypassed through HTTP Basic authentication.	2026-07-03	8.1	CVE-2026-28699
Gitea--Gitea Open Source Git Server	Gitea versions from 1.25.0 before 1.26.0 allow stored cross-site scripting through the extensionsRequired field in glTF files rendered by the 3D file viewer.	2026-07-03	8.7	CVE-2026-28737
Gitea--Gitea Open Source Git Server	Gitea versions up to and including 1.26.1 allow Git smart HTTP requests authenticated with bearer tokens to bypass repository token scope checks.	2026-07-03	8.1	CVE-2026-28744
Gitea--Gitea Open Source Git Server	Permanent Fork PR Workflow Approval Gate Bypass	2026-07-03	8.9	CVE-2026-58424
Gitea--Gitea Open Source Git Server	Gitea versions from 1.5.0 before 1.26.3 have a TOTP single-use enforcement defect that allows a valid TOTP code to be accepted more	2026-07-03	7.1	CVE-2026-20779

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	than once across web two-factor authentication flows and the Basic Auth X-Gitea-OTP path.			
Gitea--Gitea Open Source Git Server	Gitea versions up to and including 1.26.2 allow Git LFS object reuse to authorize private source objects for users who have repository access but lack Code-unit access.	2026-07-03	7.1	CVE-2026-28740
Gitea--Gitea Open Source Git Server	LFS authentication bypass via malformed SSH sub-verb allows unauthorized read access to private repositories	2026-07-03	7.7	CVE-2026-58423
GNOME--GLib	A flaw was found in GLib. An off-by-one error can occur in the g_key_file_get_locale_string_list function in the gkeyfile.c file when loading a key file with an empty value. This flaw can cause an out-of-bounds access of 1 byte or a denial of service when the out-of-bounds access crosses a page boundary.	2026-06-30	7.3	CVE-2026-58014
GNOME--GLib	A flaw was found in GLib. A state confusion issue exists in g_dbus_node_info_new_for_xml() in the gio/gdbusintrospection.c file when processing malformed D-Bus introspection XML, specifically with a <node> element nested within other elements like <method>, <signal>, <property> or <arg>. This issue can cause an unsigned integer overflow and lead to an out-of-bounds read, resulting in a denial of service.	2026-06-30	7.5	CVE-2026-58016
GoodLayers--Tourmaster	Subscriber Local File Inclusion in Tourmaster <= 5.4.5 versions.	2026-07-02	7.5	CVE-2025-69133
gorse-io--gorse	Gorse before 0.5.10 contains an authentication bypass vulnerability in the /api/dump and /api/restore endpoints that allows unauthenticated attackers to access protected functionality when admin_api_key is empty, which is the default configuration. Remote attackers can exfiltrate the entire database including user records, items, and feedback data containing personally identifiable information, or completely overwrite the dataset without authentication.	2026-06-29	9.8	CVE-2026-56782
gradio-app--gradio	Gradio before 6.16.0 contain a path traversal vulnerability in the FileExplorer component's preprocess() method that allows unauthenticated attackers to escape the configured root directory by supplying path segments containing directory traversal sequences or absolute paths. Attackers can provide crafted path segments that cause os.path.join to discard the root_dir prefix entirely, resulting in arbitrary file read or exposure of sensitive files outside the intended directory.	2026-07-01	7.5	CVE-2026-49119
Grav--Grav	Grav CMS before 2.0.0-beta.2 contains multiple code-execution vulnerabilities. Three unsafe unserialize() calls - in Scheduler\JobQueue, Framework\Cache\Adapter\FileCache, and Session - deserialize untrusted data without restricting allowed classes, enabling PHP object injection and, via a gadget chain, arbitrary code execution where an attacker controls the serialized input. Additionally, InstallCommand's git clone operation passes the branch, url, and path parameters into a shell command without escaping, allowing OS command injection via plugin/theme installation (which requires admin access). A Twig security blacklist bypass (server-side template injection) is also present. The issues are fixed in 2.0.0-beta.2.	2026-06-30	9.8	CVE-2026-56700
Greg Winiarski--WPAdverts	Unauthenticated Cross Site Scripting (XSS) in WPAdverts <= 2.3.1 versions.	2026-07-02	7.1	CVE-2026-57366
Guangzhou Red Sea Cloud Computing Co., Ltd.--Red Sea Cloud eHR	Redsea Cloud eHR contains an arbitrary file upload vulnerability that allows unauthenticated attackers to achieve remote code execution by uploading malicious files through the PtFjk.mob servlet endpoint. Attackers can submit a multipart POST request with a JSP webshell disguised using a spoofed image/jpeg Content-Type to bypass the absence of extension and MIME type validation, with the uploaded file stored at a predictable path under the uploadfile directory and executed directly by the web server. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-11-03 (UTC).	2026-07-02	9.8	CVE-2024-14037
guardian--language-system	Guardian language-system passes the id GET parameter directly into an unsanitized SQL query in job_info.php (line 16): SELECT * FROM jobs where id = \".\$_GET['id'].\". No authentication is required. An	2026-07-01	9.8	CVE-2026-34099

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthenticated attacker can perform error-based SQL injection to extract the database version, current user, schema names, and table contents.			
guardian--language-system	Guardian language-system passes the id GET parameter directly into an unsanitized SQL query in media.php (line 17): SELECT id, filename, extension, type, duration, owner, private FROM files where id = \"\$_GET['id']\". An authenticated attacker can perform error-based SQL injection to extract database contents.	2026-07-01	9.8	CVE-2026-34100
guardian--language-system	Guardian language-system passes the id GET parameter directly into an unsanitized SQL query in text_file.php (line 17): SELECT id, filename, extension, type, duration, owner, private FROM files where id = \"\$_GET['id']\". An authenticated attacker can perform error-based SQL injection to extract database contents.	2026-07-01	9.8	CVE-2026-34101
guardian--language-system	Guardian language-system passes the id GET parameter directly into an unsanitized SQL query in job_info_get.php (line 16): SELECT * FROM jobs where input1 = \"\$_GET['id']\". An authenticated attacker can perform error-based SQL injection to extract database contents.	2026-07-01	9.8	CVE-2026-34102
guardian--language-system	Guardian language-system passes the id GET parameter directly into an unsanitized SQL query in subtitles.php (line 16): SELECT id, filename, extension, type FROM files where id = \"\$_GET['id']\". An authenticated attacker can perform error-based SQL injection to extract database contents.	2026-07-01	9.8	CVE-2026-34103
guardian--language-system	Guardian language-system passes the name GET parameter directly into an unsanitized SQL query in designer.php (line 124): SELECT * FROM complex WHERE name= \"\$_GET['name']\". An authenticated attacker can perform error-based SQL injection to extract database contents.	2026-07-01	9.8	CVE-2026-34104
guardian--language-system	Guardian language-system passes the id GET parameter directly into an unsanitized SQL query in translate_text.php (line 15): SELECT id, filename, extension, type FROM files where id = \"\$_GET['id']\". An authenticated attacker can perform error-based SQL injection to extract database contents.	2026-07-01	9.8	CVE-2026-34105
guardian--language-system	Guardian language-system passes the id GET parameter directly into a PHP exec() call in subtitles.php (line 19) without sanitization: exec(\"php jobs/subtitle_rendering.php \".\$login_session.\" \"\$_GET['id']\" ...\". No authentication is required. An unauthenticated remote attacker can append shell metacharacters to the id parameter to execute arbitrary OS commands on the server.	2026-07-01	9.8	CVE-2026-34106
guardian--language-system	Guardian language-system passes the id GET parameter directly into a PHP exec() call in translate.php (line 14) without sanitization: exec(\"php jobs/translate.php \".\$login_session.\" \"\$_GET['id']\" ...\". No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	2026-07-01	9.8	CVE-2026-34107
guardian--language-system	Guardian language-system passes the id GET parameter directly into a PHP exec() call in text.php (line 15) without sanitization: exec(\"php jobs/text.php \".\$login_session.\" \"\$_GET['id']\" ...\". No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	2026-07-01	9.8	CVE-2026-34108
guardian--language-system	Guardian language-system passes the id GET parameter directly into a PHP exec() call in speech.php (line 18) without sanitization: exec(\"php jobs/speech_audio.php \".\$login_session.\" \"\$_GET['id']\" ...\". No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	2026-07-01	9.8	CVE-2026-34109
guardian--language-system	Guardian language-system passes the id GET parameter directly into a PHP exec() call in complex_start.php (line 14) without sanitization: exec(\"php jobs/complex.php \".\$login_session.\" \"\$_GET['id']\" ...\". No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	2026-07-01	9.8	CVE-2026-34110

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
guardian--language-system	Guardian language-system passes the id GET parameter directly into a PHP exec() call in speechmac_text.php (line 18) without sanitization: exec(\"php jobs/speech_audio_mac_text.php \". \$login_session.\" \"\$_GET['id'].\" ... \"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	2026-07-01	9.8	CVE-2026-34111
guardian--language-system	Guardian language-system passes the id GET parameter directly into a PHP exec() call in speechmac.php (line 18) without sanitization: exec(\"php jobs/speech_audio_mac.php \". \$login_session.\" \"\$_GET['id'].\" ... \"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	2026-07-01	9.8	CVE-2026-34112
guardian--language-system	Guardian language-system passes the id GET parameter directly into a PHP exec() call in speech_text.php (line 18) without sanitization: exec(\"php jobs/speech_audio_text.php \". \$login_session.\" \"\$_GET['id'].\" ... \"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	2026-07-01	9.8	CVE-2026-34113
guardian--language-system	Guardian language-system passes the id GET parameter directly into a PHP exec() call in translate_text.php (line 18) without sanitization: exec(\"php jobs/translate_text.php \". \$login_session.\" \"\$_GET['id'].\" ... \"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	2026-07-01	9.8	CVE-2026-34114
guardian--language-system	Guardian language-system passes the id GET parameter directly into a PHP exec() call in transcribe_amazon.php (line 15) without sanitization: exec(\"php jobs/transcribe_amazon.php \". \$login_session.\" \"\$_GET['id'].\" ... \"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	2026-07-01	9.8	CVE-2026-34115
guardian--language-system	Guardian language-system passes the id GET parameter directly into a PHP exec() call in transcribe.php (line 15) without sanitization: exec(\"php jobs/transcribe.php \". \$login_session.\" \"\$_GET['id'].\" ... \"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	2026-07-01	9.8	CVE-2026-34116
guardian--language-system	Guardian language-system passes the id GET parameter directly into a PHP exec() call in text_to_subtitles.php (line 19) without sanitization: exec(\"php jobs/text_to_subtitles.php \". \$login_session.\" \"\$_GET['id'].\" ... \"). No authentication is required. An unauthenticated remote attacker can append shell metacharacters to execute arbitrary OS commands on the server.	2026-07-01	9.8	CVE-2026-34117
Gurmehub--POS Integratr	Unauthenticated Broken Access Control in POS Integratr Å¶r <= 3.7.103 versions.	2026-07-02	8.2	CVE-2026-57688
Haktan Suren--HandL UTM Grabber	Unauthenticated Cross Site Scripting (XSS) in HandL UTM Grabber <= 2.9.2 versions.	2026-07-02	7.1	CVE-2026-57351
Hanwang--e-Face General Management Platform	A vulnerability was determined in Hanwang e-Face General Management Platform 6.3.5.4. This issue affects some unknown processing of the file /manage/resourceUpload/upload.do. Executing a manipulation of the argument File can lead to unrestricted upload. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized.	2026-06-29	7.3	CVE-2026-13547
Hanwang--e-Face General Management Platform	A vulnerability was identified in Hanwang e-Face General Management Platform 6.3.5.4. This impacts an unknown function of the file /sysAuthStr/querySysAuthStr.do. The manipulation of the argument order leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	2026-07-05	7.3	CVE-2026-14737
Heateor Support--	Unauthenticated Cross Site Request Forgery (CSRF) in Heateor Social Login <= 1.1.39 versions.	2026-07-02	8.1	CVE-2026-57751

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Heateor Social Login				
Hiroaki Miyashita--Custom Field Template	Contributor SQL Injection in Custom Field Template <= 2.7.8 versions.	2026-07-02	8.5	CVE-2026-57687
Hitachi--Hitachi Virtual Storage Platform E390, E590, E790, E990, E1090, E390H, E590H, E790H, E1090H	Improper Authorization Vulnerability of Maintenance Utility in Hitachi Virtual Storage Platform. This issue affects Hitachi Virtual Storage Platform E390, E590, E790, E990, E1090, E390H, E590H, E790H, E1090H: before DKCMAIN Ver. 93-07-26-xx/00, GUM Ver. 93-07-26/00; Hitachi Virtual Storage Platform 5100, 5500, 5100H, 5500H, 5200, 5600, 5200H, 5600H: before DKCMAIN Ver. 90-09-27-00/00, GUM Ver. 90-09-27/00; Hitachi Virtual Storage Platform G130, G150, G350, G370, G700, G900, F350, F370, F700, F900: before DKCMAIN Ver. 88-08-16-xx/00, GUM Ver. 88-08-20/00.	2026-06-29	8.3	CVE-2025-2902
hiyouga--LlamaFactory	LLaMA-Factory through 0.9.5 contains a remote code execution vulnerability that allows attackers with WebUI access to execute arbitrary Python code by supplying a malicious model path in the Chat or Training interfaces. The application passes user-supplied model path input unvalidated into AutoTokenizer.from_pretrained() and AutoModel.from_pretrained() with a hardcoded trust_remote_code=True parameter, causing the Hugging Face transformers library to fetch and execute arbitrary code from a remote or local model repository with the privileges of the server process.	2026-06-30	9.8	CVE-2026-58116
HKUDS--DeepTutor	DeepTutor before version 1.4.10 contains an authorization bypass vulnerability that allows low-privilege users to invoke unrestricted MCP tools due to the allowed_mcp_tools function returning None instead of a denied result when mcp_tools is omitted from a user's grant in deeptutor/multi_user/tool_access.py. Attackers or prompt-injected content acting within a user session can enumerate and invoke any configured MCP tool, including filesystem, shell, and browser servers, gaining unauthorized access to sensitive deployment resources.	2026-06-30	8.8	CVE-2026-58168
HKUDS--Vibe-Trading	Vibe-Trading before 0.1.10 builds the proposal file path by joining a caller-supplied proposal identifier onto the broker proposals directory without sanitization (agent/src/live/mandate/commit.py). A proposal identifier containing path traversal sequences causes the application to load an attacker-controlled JSON file as an authoritative live trading mandate. Combined with the file upload endpoint, an admitted caller can write a JSON file to a known location and traverse to it, and because the ceilings validation is skipped when ceilings are absent, the attacker fully controls the committed mandate.	2026-06-30	8.3	CVE-2026-58170
HKUDS--Vibe-Trading	Vibe-Trading before 0.1.10 contains a DNS rebinding authentication bypass vulnerability that allows remote attackers to bypass bearer-token authentication by exploiting the server's trust of TCP peer addresses for loopback clients combined with missing Host header validation while binding to 0.0.0.0 with credentialed CORS. Attackers can craft a malicious DNS rebinding page to issue authenticated requests to the local API server, reach the shell execution endpoint with a bash-enabled preset, and achieve remote code execution as the API process user while also overwriting LLM and data-source settings to exfiltrate credentials.	2026-06-30	7.5	CVE-2026-58169
home-assistant--core	Home Assistant is open source home automation software that puts local control and privacy first. Prior to 2025.5.0, The iOS companion app ignores the SSID allowlist for internal networks. The app uses SSID to detect when to use the internal URL, but whenever the app cannot find any other URL to be used, it fallbacks to the internal URL as well, which can expose user's token when connected to a not secure network. This vulnerability is fixed in 2025.5.0.	2026-06-29	7.5	CVE-2026-55844
hoppscotch--hoppscotch	Hoppscotch is an API development ecosystem. In self-hosted deployments of hoppscotch-backend from version 2026.4.1 and earlier, the unauthenticated POST /v1/onboarding/config endpoint is vulnerable to	2026-07-01	10	CVE-2026-50160

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	mass assignment. The global NestJS ValidationPipe is configured without whitelist: true, so extra properties on the request body that are not declared in SaveOnboardingConfigRequest are not stripped and are iterated in the service layer as if they were legitimate InfraConfig entries. Because keys such as JWT_SECRET and SESSION_SECRET are valid InfraConfigEnum values and are not explicitly rejected during validation, an unauthenticated attacker who can reach a fresh instance before onboarding completes (or when no users exist) can overwrite these values in the database. Overwriting JWT_SECRET gives the attacker control of the JWT signing key, allowing them to forge tokens for any user, including administrators, and results in full server compromise. The issue is fixed in hoppscotch 2026.5.0.			
https://wpreviewslider.com/--WP-Review-Slider-Pro	The WP Review Slider Pro plugin for WordPress is vulnerable to SQL Injection via the 'notinstring' parameter of the wprp_load_more_revs AJAX action in versions up to, and including, 12.7.2. The parameter is read via \$_POST['notinstring'] and passed through sanitize_text_field() - which strips HTML and whitespace but does not provide SQL safety. The value is then concatenated directly into a numeric/unquoted 'AND id NOT IN (...)' clause and executed via \$wpdb->get_results() without \$wpdb->prepare() or intval() casting. Because the value sits in an unquoted numeric context, WordPress's wp_magic_quotes protection (which only escapes embedded quotes) is ineffective. The AJAX hook is registered via wp_ajax_nopriv_wprp_load_more_revs, and the required check_ajax_referer nonce is publicly available via wp_localize_script on any frontend page that renders the plugin shortcode, so an unauthenticated attacker who can reach a public page hosting the plugin can extract arbitrary data from the database via blind/time-based injection.	2026-07-02	7.5	CVE-2026-8441
HubSpot--HubSpot	Insertion of Sensitive Information Into Sent Data vulnerability in HubSpot allows Retrieve Embedded Sensitive Data. This issue affects HubSpot: from n/a through 11.3.51.	2026-07-01	7.4	CVE-2026-57736
Hyland--PACSGear MediaWriter	PACSGear MediaWriter 5.2.1 exposes a .NET Remoting TCP service on port 9000 via PacsgearMediaServerEngine.dll, registered with ObjectURIs RemoteObj and UIRemoteObj, without any authentication requirement. By exploiting the MarshalByRefObject object unmarshalling technique and implementing .NET WebClient class methods, an unauthenticated remote attacker can read and write arbitrary files on the host filesystem. The ObjectURIs are identical across all installations by default. Chaining the arbitrary file write primitive with DLL hijacking opportunities in the MediaWriter service (which runs as NT Authority\SYSTEM and loads missing DLLs such as CRYPTBASE.DLL from the application directory) enables unauthenticated remote code execution as SYSTEM upon service restart.	2026-07-01	9.8	CVE-2026-58127
Hyland--PACSGear PACS Scan	PACSGear PACS Scan 5.2.1 contains an unauthenticated remote code execution vulnerability that allows remote attackers to read and write arbitrary files by exploiting an exposed .NET Remoting TCP service on port 22222 via PGImageExchQueue.exe without any authentication requirement. Attackers can chain the arbitrary file write primitive with DLL hijacking in PGImageExchangeQueueSvc.exe, which loads missing DLLs such as CRYPTSP.DLL from the application directory, to achieve remote code execution as NT Authority\SYSTEM upon service restart.	2026-07-01	9.8	CVE-2026-58126
IBM--Business Automation Manager Open Editions	IBM Business Automation Manager Open Editions 9.0.0 through 9.4.2 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	2026-06-30	7.6	CVE-2026-13449
IBM--Db2	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 is vulnerable to remote code execution due to improper pre-auth DRDA handshake handling.	2026-06-30	9.8	CVE-2026-10109

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--DevOps Automation	IBM DevOps Automation 1.0.1 and IBM DevOps Loop 1.0.2 does not invalidate session IDs after expiration which could allow an authenticated user to impersonate another user on the system.	2026-06-30	8.1	CVE-2025-36359
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.9.3 allows an attacker to read every secret available to the Langflow process, read and modify every flow, conversation, message, file upload, and saved component in the Langflow database, can connect to internal services, abuse cloud metadata endpoints, laterally move to other tenants on the same Langflow instance, and Establish persistence by modifying the public flow's `tool_code` so normal `/api/v1/build/...` calls by any user re-execute attacker code at each build.	2026-06-30	10	CVE-2026-10134
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.0 voice mode contains improper shared-state handling that allows reuse of API clients across tenant boundaries. An authenticated attacker can manipulate cache state to cause requests from other users to be processed using incorrect upstream API credentials, leading to cross-tenant billing and accountability misattribution.	2026-06-30	9.6	CVE-2026-10140
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.9.6 could allow unauthenticated attackers to access protected MCP project resources and execute MCP operations due to improper authorization enforcement in the Streamable MCP transport endpoint.	2026-06-30	9.1	CVE-2026-7663
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.0 could allow arbitrary code execution due to improper validation of flow nodes with missing or empty component type fields.	2026-06-30	9.8	CVE-2026-7803
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.0 allows users with Redis access to execute arbitrary code with full application privileges, compromising all secrets, data, and system integrity.	2026-06-30	9.8	CVE-2026-7871
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.0 allows authenticated attackers to execute arbitrary OS commands and read sensitive files including credentials, enabling complete system compromise and lateral movement.	2026-06-30	9.9	CVE-2026-7873
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.10.0 Langflow could allow disclosure of all stored credentials due to the use of a weak and reversible key derivation mechanism for encryption at rest.	2026-06-30	9.1	CVE-2026-7874
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.9.3 contains a Server-Side Request Forgery (SSRF) protection bypass vulnerability in the API Request component. An authenticated attacker with low-level privileges (flow author role) can bypass SSRF protections by enabling the follow_redirects parameter and supplying a public URL that redirects to internal/localhost addresses. The vulnerability exists because the application validates only the initial URL but does not re-validate redirect destinations. This allows attackers to access internal HTTP services, localhost endpoints, cloud metadata services, and private network resources that should be unreachable when SSRF protection is enabled. Successful exploitation can lead to disclosure of sensitive information including credentials, tokens, internal API responses, and administrative panel data.	2026-06-30	8.5	CVE-2026-10129
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.9.6 contains a missing authentication vulnerability in /api/v1/build_public_tmp/ endpoints that allows an unauthenticated attacker to read build event data or cancel jobs using a valid job identifier, resulting in information disclosure and denial of service.	2026-06-30	8.2	CVE-2026-10560
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.9.6 contains a Server-Side Request Forgery (SSRF). The legacy RSSReaderComponent in rss.py and SearXNG component in searxng.py make unvalidated HTTP requests to user-controlled URLs, bypassing SSRF protections introduced in version 1.9.3. An authenticated attacker can exploit this to access internal resources including cloud metadata services (AWS/Azure/GCP IMDS), potentially exfiltrating IAM credentials and enumerating internal networks. The vulnerability can also be triggered through prompt injection in agentic workflows due to tool_mode=True exposure.	2026-06-30	8.2	CVE-2026-10564

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--Langflow OSS	IBM Langflow OSS 1.0.0 through 1.9.3 contains a Server-Side Request Forgery (SSRF) vulnerability in the URL component (src/lfx/src/lfx/components/data_source/url.py) due to a Time-of-Check/Time-of-Use (TOCTOU) race condition that can be exploited via DNS rebinding.	2026-06-30	7.1	CVE-2026-10546
IBM--WebSphere Application Server	IBM WebSphere Application Server 9.0, and 8.5 is affected by a cross-site scripting vulnerability in the administrative console's integrated help system.	2026-06-30	9.3	CVE-2026-11708
IBM--WebSphere Application Server	IBM WebSphere Application Server 9.0, and 8.5 is affected by a cross-site scripting vulnerability in the administrative console help system.	2026-06-30	9.3	CVE-2026-11712
IBM--WebSphere Application Server	IBM WebSphere Application Server 9.0, and 8.5 is affected by a cross-site scripting vulnerability in the administrative console.	2026-06-30	8.5	CVE-2026-11594
IBM--WebSphere Application Server	IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.6 are affected by an HTTP request smuggling vulnerability.	2026-06-30	7.4	CVE-2026-11541
IBM--WebSphere Application Server - Liberty	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 is affected by a server-side request forgery vulnerability with the apiDiscovery-1.0 feature enabled.	2026-06-30	8.5	CVE-2026-11714
IBM--WebSphere Application Server - Liberty	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 is affected by a server-side request forgery vulnerability with the adminCenter-1.0 feature enabled.	2026-06-30	7.1	CVE-2026-11546
IBM--WebSphere Application Server - Liberty	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.6 is affected by an arbitrary file read vulnerability with the restConnector-2.0 feature enabled.	2026-06-30	7.2	CVE-2026-11806
IBM--WebSphere Extreme Scale	IBM WebSphere Extreme Scale 8.6.1.0 through 8.6.1.6 ships three ObjectInputStream subclasses (WsObjectInputStream, ObjectStreamPool\$ReusableInputStream, ObjectInputStreamResolver) that install no JEP-290 class filter; when Coherence is on the classpath, multiple RCE gadget chains including RemoteConstructor.readResolve and PriorityQueue/ExtractorComparator are confirmed working, allowing a post-login attacker who can write a session attribute or a LAN-adjacent attacker on the grid replication wire to execute arbitrary code on peer WAS JVMs	2026-06-30	7.5	CVE-2026-13759
IBM--WebSphere Extreme Scale	IBM WebSphere Extreme Scale 8.6.1.0 through 8.6.1.6's Object Query Language engine resolves attacker-supplied class names via Class.forName() and invokes their constructors with no allow-list at three distinct sinks (SELECT NEW, enum literals, and reflection-based comparators); an authenticated remote attacker who can influence an application-built OQL query string can execute arbitrary constructors on the WAS JVM, and a SELECT DISTINCT variant using planted grid values fires the same gadget post-readObject in a manner that survives JEP-290 serialization filters across grid node boundaries	2026-06-30	7.5	CVE-2026-13772
imithemes--NativeChurch	Unauthenticated Cross Site Scripting (XSS) in NativeChurch <= 4.8.8.2 versions.	2026-07-02	7.1	CVE-2026-27408
impleCode--eCommerce Product Catalog	Unauthenticated Cross Site Scripting (XSS) in eCommerce Product Catalog <= 3.5.4 versions.	2026-07-02	7.1	CVE-2026-57360
iNET--iNET Webkit	Contributor SQL Injection in iNET Webkit 1.2.4 versions.	2026-07-02	8.5	CVE-2026-57752
itsourcecode--Baptism Information Management System	A weakness has been identified in itsourcecode Baptism Information Management System 1.0. The impacted element is an unknown function of the file /delbaptism.php. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	2026-06-29	7.3	CVE-2026-13550
itsourcecode--Baptism	A security vulnerability has been detected in itsourcecode Baptism Information Management System 1.0. This affects an unknown function of	2026-06-29	7.3	CVE-2026-13551

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Information Management System	the file /editBaptism.php. Such manipulation of the argument ID leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.			
itsourcecode--Online Hotel Management System	A vulnerability was detected in itsourcecode Online Hotel Management System 1.0. This impacts an unknown function of the file /admin/mod_amenities/controller.php?action=edit. Performing a manipulation of the argument amen_id results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	2026-06-29	7.3	CVE-2026-13552
itsourcecode--Online Hotel Management System	A flaw has been found in itsourcecode Online Hotel Management System 1.0. Affected is an unknown function of the file /admin/mod_amenities/controller.php?action=add. Executing a manipulation of the argument image can lead to unrestricted upload. It is possible to launch the attack remotely. The exploit has been published and may be used.	2026-06-29	7.3	CVE-2026-13553
itsourcecode--Online Hotel Management System	A vulnerability was found in itsourcecode Online Hotel Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/mod_users/controller.php?action=add. The manipulation of the argument Name results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	2026-06-29	7.3	CVE-2026-13555
itsourcecode--Online Hotel Management System	A vulnerability was identified in itsourcecode Online Hotel Management System 1.0. The affected element is an unknown function of the file /admin/login.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	2026-07-05	7.3	CVE-2026-14688
Jacob N. Breetvelt--WP Photo Album Plus	Unauthenticated Cross Site Scripting (XSS) in WP Photo Album Plus <= 9.2.02.004 versions.	2026-07-02	7.1	CVE-2026-57675
JAIoTlink--C492A-W6 Wi-Fi IP Camera	JAIoTlink C492A-W6 Wi-Fi IP cameras running firmware 4.8.30.57701411 contain a hard-coded credentials vulnerability that allows network-adjacent attackers to gain unauthorized access by using the default admin username with an empty password accepted by the anyka_ipc HTTP service on port 80. Attackers can authenticate with these hardcoded credentials to access camera snapshots, video streams, network configuration, and factory-level API endpoints including the SetMAC command injection surface.	2026-07-01	9.8	CVE-2026-58453
JAIoTlink--C492A-W6 Wi-Fi IP Camera	JAIoTlink C492A-W6 Wi-Fi IP cameras running firmware 4.8.30.57701411 contain an OS command injection vulnerability that allows authenticated attackers to achieve remote code execution by supplying a malicious Wireless parameter to the HTTP PUT NetSDK/Factory SetMAC endpoint. Attackers can craft a string beginning with a valid MAC-like prefix followed by a semicolon and a shell payload, which bypasses partial sscanf() validation and is passed unsanitized into an echo shell command executed through a system() wrapper.	2026-07-01	8.8	CVE-2026-58452
JAIoTlink--C492A-W6 Wi-Fi IP Camera	JAIoTlink C492A-W6 Wi-Fi IP cameras running firmware 4.8.30.57701411 contain a remote code execution vulnerability that allows authenticated attackers to execute arbitrary shell scripts by writing to the writable persistent JFFS2 storage path and triggering execution through the authenticated HTTP endpoint. Attackers can stage a malicious script in the writable persistent storage and request the config endpoint to invoke it via popen(), achieving persistent remote code execution that survives device reboots.	2026-07-01	7.5	CVE-2026-58454
jairiidriss--restaurant-website-php-mysql	A vulnerability was found in jairiidriss restaurant-website-php-mysql up to 521428b5b612449df0cf4a5d15ee40cba67f3d35. This vulnerability affects unknown code of the file /admin/ajax_files of the component AJAX Endpoint. Performing a manipulation results in missing authentication. The attack is possible to be carried out remotely. The exploit has been made public and could be used. This product adopts a rolling release strategy to	2026-07-04	7.3	CVE-2026-14622

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.			
jeecgboot--JeecgBoot	JeecgBoot through 3.9.2 contains a broken access control vulnerability that allows authenticated low-privilege users to perform full create, read, update, and delete operations on OpenAPI credentials by accessing the OpenApiAuthController and OpenApiPermissionController endpoints which lack Shiro authorization annotations. Attackers can exploit the unenforced access controls to list, add, edit, and delete all AK/SK credential pairs, with the list endpoint returning secret keys in plaintext, enabling credential theft and unauthorized invocation of the OpenAPI surface.	2026-06-30	8.1	CVE-2026-58377
jeecgboot--jimureport	JimuReport through 2.5.0 exposes the POST /jmreport/auto/export endpoint without authentication: the handler is annotated @JimuNoLoginRequired, so JimuReportTokenInterceptor skips all authentication and authorization, and the export service streams the rendered report for any supplied report id without verifying the auto-export configuration flag. An unauthenticated remote attacker can enumerate Snowflake report identifiers and export the full contents of any report, including the data returned by the report configured SQL queries and any credentials embedded in its data sources.	2026-06-30	7.5	CVE-2026-58375
juicedata--juicefs	JuiceFS through 1.3.1, fixed in commit a46979c, contains an authentication bypass vulnerability that allows unauthenticated remote attackers to access sensitive debug and metrics endpoints by exploiting improper handler registration on the shared http.DefaultServeMux. Attackers can request the /debug/pprof/cmdline endpoint to obtain the process command line containing metadata engine connection strings with database credentials, granting full read/write access to filesystem metadata, while other pprof handlers leak internal state and profiling handlers enable denial of service.	2026-07-02	7.7	CVE-2026-59092
kirilkirkov--Ecommerce-Codelgniter-Bootstrap	A security vulnerability has been detected in kirilkirkov Ecommerce-Codelgniter-Bootstrap up to 13fd582aaf49aeab7438acc0fc3eb973a1f5e6a7. The affected element is the function getCartItems in the library application/libraries/ShoppingCart.php. The manipulation of the argument shopping_cart leads to deserialization. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. Continuous delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The identifier of the patch is 49b20f53de2b7ec34e920b11c863f1491d911a04. It is recommended to apply a patch to fix this issue.	2026-07-04	8.2	CVE-2026-14637
kirilkirkov--Ecommerce-Codelgniter-Bootstrap	A security flaw has been discovered in kirilkirkov Ecommerce-Codelgniter-Bootstrap up to 222ff31c06687b1c6d0e1ab63953f82c3674c52b. This issue affects some unknown processing of the file application/modules/vendor/controllers/AddProduct.php of the component Vendor Multi-Image Endpoint. Performing a manipulation of the argument folder results in path traversal. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. This product is using a rolling release to provide continuous delivery. Therefore, no version details for affected nor updated releases are available. The patch is named 2a9497ff11f36e573ad99e1c357ff0e6ded49745. Applying a patch is the recommended action to fix this issue.	2026-07-04	7.3	CVE-2026-14635
KongHQ--mcp-konnect	A vulnerability exists in the Kong Konnect Model Context Protocol (MCP) server prior to version 1.0.0, which could allow a remote attacker to perform an indirect prompt injection attack and execute unintended API requests.	2026-07-03	7.4	CVE-2026-13341
kstover--Ninja Forms The	The Ninja Forms - The Contact Form Builder That Grows With You plugin for WordPress is vulnerable to unauthorized access of data due to a	2026-07-01	7.5	CVE-2026-1239

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Contact Form Builder That Grows With You	missing authorization check on the 'ninja-forms-views/token/refresh' REST callback in all versions up to, and including, 3.14.1. This makes it possible for unauthenticated attackers to view form submissions, which could potentially contain sensitive information.			
LadybirdBrowser --Ladybird	Ladybird contains a dangling-reference memory-safety flaw in its WebAssembly ESM-integration module loader. When a JavaScript function is imported into a WebAssembly module via the ESM path, WebAssemblyModule.cpp passes a stack-local Wasm::FunctionType by reference to create_host_function, whose host callback captures and later reads that reference; once the ESM link-loop iteration ends the FunctionType is destroyed, leaving the callback with a dangling reference (the normal instantiate path uses a long-lived reference and is not affected). Stale result-type data lets the host callback return an empty result vector for a statically non-empty result, so the destination register retains an attacker-influenced value that is then consumed by the WASM-GC array.set handler, which bit-casts the reference low bits to an ArrayInstance pointer after only a null check, yielding an arbitrary write. A web page can chain this into code execution in the WebContent process. Verified reachable from HTML content without any instrumentation or source modification.	2026-07-01	8.3	CVE-2026-58592
latepoint--LatePoint Calendar Booking Plugin for Appointments and Events	The LatePoint - Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Privilege Escalation to Administrator in versions up to, and including, 5.6.3 This is due to an Insecure Direct Object Reference (IDOR) in the create_or_update() function of OsOrdersController, which allows an authenticated Agent to supply an arbitrary order[customer_id] and overwrite any LatePoint customer's email field (including one linked to a WordPress Administrator's account) through the public-scope customer set_data() call, combined with a missing role verification in OsAuthHelper::authorize_customer() which logs in the linked WordPress user without checking its role. This makes it possible for authenticated attackers, with custom (Agent)-level access and above, to elevate their privileges to Administrator.	2026-07-01	8.8	CVE-2026-13228
LCweb--PrivateContent	Incorrect Privilege Assignment vulnerability in LCweb PrivateContent allows Privilege Escalation. This issue affects PrivateContent: from n/a through 9.9.2.	2026-07-01	9.8	CVE-2026-57692
leshchenko1979--fast-mcp-telegram	fast-mcp-telegram is a Telegram MCP Server. Prior to 0.19.1, fast-mcp-telegram validates HTTP Bearer tokens by joining the raw token string into a session-file path. The verifier rejects the exact reserved token telegram, but it does not reject path separators or normalize the path before checking whether the session file exists. A remote HTTP client can therefore authenticate as the default legacy session with a token such as ../fast-mcp-telegram/telegram when the documented default session file ~/.config/fast-mcp-telegram/telegram.session exists. This bypasses the reserved session name control that is intended to prevent HTTP multi-user sessions from colliding with the default stdio or legacy account. With account-prefixed MCP tools enabled, the attacker still sees and calls the prefixed tools for the default account, so the prefix middleware does not stop the session selection bypass. This vulnerability is fixed in 0.19.1.	2026-07-02	9.4	CVE-2026-52830
Levelfourdevelopment--WP EasyCart	Contributor SQL Injection in WP EasyCart <= 5.9.0 versions.	2026-07-02	8.5	CVE-2026-57765
liftoff-sr--CIPster	A vulnerability was detected in liftoff-sr CIPster up to e8e9dba09bf56962807d3504b783ccdb6287f3e4. Affected by this issue is the function BufWriter::append of the component EtherNet IP Message Handler. Performing a manipulation results in out-of-bounds write. Remote exploitation of the attack is possible. The exploit is now public and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The patch is named	2026-06-29	7.3	CVE-2026-13592

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	3a0159ed43125dcd024a1965f0289cb186bae9ff. To fix this issue, it is recommended to deploy a patch.			
LinuxCNC--LinuxCNC	rtapi_app in linuxcnc-usrpace in LinuxCNC before 2.9.9 allows privilege escalation. It is installed SUID root and loads shared library modules via dlopen() by using a user-supplied module name. Insufficient validation of the module name allows path traversal, enabling an unprivileged local user to load an arbitrary shared library. Because the process retains elevated privileges during module loading, this results in local privilege escalation to root.	2026-06-30	8.4	CVE-2026-58302
lobehub--lobehub	LobeChat before 2.2.10-canary.18 contains a server-side request forgery vulnerability that allows authenticated attackers to direct internal HTTP requests to arbitrary URLs by supplying user-controlled input to the skill import service (importFromUrl) and topic cover update (fetchImageFromUrl) endpoints, which use the global fetch without the project's ssrf-safe-fetch wrapper. Attackers can target internal addresses such as cloud instance metadata endpoints through these unprotected code paths to disclose internal service responses and cloud credentials.	2026-07-02	7.7	CVE-2026-59095
Melograno Venture Studio--wpDataTables	Unauthenticated Cross Site Scripting (XSS) in wpDataTables <= 6.5.1.1 versions.	2026-07-02	7.1	CVE-2026-57672
Merkulove--OpenAI Chatbot for WordPress Helper	Unauthenticated Arbitrary Content Deletion in OpenAI Chatbot for WordPress - Helper <= 1.1.4 versions.	2026-07-02	7.5	CVE-2025-69134
Metagauss--ProfileGrid	Unauthenticated Cross Site Request Forgery (CSRF) in ProfileGrid <= 5.9.9.7 versions.	2026-07-02	8.8	CVE-2026-57759
metagauss--ProfileGrid User Profiles, Groups and Communities	The ProfileGrid - User Profiles, Groups and Communities plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 5.9.9.5. This is due to the plugin not validating a `user_login` on registration forms that don't contain this parameter, and not properly handling the error messages. This makes it possible for unauthenticated attackers to change email address of user account with ID=1 (usually an administrator), and leverage that to reset the user's password and gain access to their account.	2026-06-30	9.8	CVE-2026-12073
metagauss--RegistrationMagic Custom Registration Forms, User Registration, Payment, and User Login	The RegistrationMagic - User Registration Forms Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.0.9.1. This is due to missing or incorrect nonce validation on the process_request function. This makes it possible for unauthenticated attackers to escalate the privileges of an arbitrary form submitter to administrator by creating a malicious Chronos automation task that is executed via WordPress cron via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-07-01	8.8	CVE-2026-12158
Microsoft--Azure Open AI	Server-side request forgery (ssrf) in Azure OpenAI allows an authorized attacker to elevate privileges over a network.	2026-07-02	9.9	CVE-2026-45499
Microsoft--Microsoft 365 Copilot	Url redirection to untrusted site ('open redirect') in M365 Copilot allows an unauthorized attacker to elevate privileges over a network.	2026-07-02	9.3	CVE-2026-41106
Microsoft--Microsoft Edge (Chromium-based)	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	9	CVE-2026-58289
Microsoft--Microsoft Edge (Chromium-based)	Use after free in Microsoft Edge (Chromium-based) allows an authorized attacker to execute code over a network.	2026-07-01	8.3	CVE-2026-50521
Microsoft--Microsoft Edge	Heap-based buffer overflow in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	8.8	CVE-2026-56645

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
(Chromium-based)				
Microsoft--Microsoft Edge (Chromium-based)	Integer overflow or wraparound in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	8.8	CVE-2026-57974
Microsoft--Microsoft Edge (Chromium-based)	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	8.8	CVE-2026-57981
Microsoft--Microsoft Edge (Chromium-based)	Improper authorization in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature over a network.	2026-07-03	8.7	CVE-2026-57983
Microsoft--Microsoft Edge (Chromium-based)	Improper access control in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-07-03	8.1	CVE-2026-58282
Microsoft--Microsoft Edge (Chromium-based)	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-07-03	8.1	CVE-2026-58283
Microsoft--Microsoft Edge (Chromium-based)	Improper authorization in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	8.3	CVE-2026-58284
Microsoft--Microsoft Edge (Chromium-based)	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	8.3	CVE-2026-58285
Microsoft--Microsoft Edge (Chromium-based)	Improper access control in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-07-03	8.1	CVE-2026-58286
Microsoft--Microsoft Edge (Chromium-based)	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	8.3	CVE-2026-58287
Microsoft--Microsoft Edge (Chromium-based)	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	8.3	CVE-2026-58288
Microsoft--Microsoft Edge (Chromium-based)	External control of file name or path in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	8.1	CVE-2026-58293
Microsoft--Microsoft Edge (Chromium-based)	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature over a network.	2026-07-03	8.3	CVE-2026-58295
Microsoft--Microsoft Edge (Chromium-based)	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	7.5	CVE-2026-57975
Microsoft--Microsoft Edge (Chromium-based)	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-07-03	7.1	CVE-2026-57977

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft-- Microsoft Edge (Chromium-based)	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	7.5	CVE-2026-57984
Microsoft-- Microsoft Edge (Chromium-based)	Improper input validation in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	7.6	CVE-2026-57985
Microsoft-- Microsoft Edge (Chromium-based)	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	7.5	CVE-2026-57986
Microsoft-- Microsoft Edge (Chromium-based)	Relative path traversal in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	7.1	CVE-2026-57988
Microsoft-- Microsoft Edge (Chromium-based)	Improper link resolution before file access ('link following') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	2026-07-03	7.4	CVE-2026-57991
Microsoft-- Microsoft Edge (Chromium-based)	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	7.5	CVE-2026-57992
Microsoft-- Microsoft Edge (Chromium-based)	Server-side request forgery (ssrf) in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-07-03	7.4	CVE-2026-57993
Microsoft-- Microsoft Edge (Chromium-based)	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	7.5	CVE-2026-58276
Microsoft-- Microsoft Edge (Chromium-based)	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	7.5	CVE-2026-58290
Microsoft-- Microsoft Edge (Chromium-based)	Improper input validation in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	7.5	CVE-2026-58292
Microsoft-- Microsoft Edge (Chromium-based)	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	2026-07-03	7.5	CVE-2026-58294
Microsoft-- Microsoft Edge (Chromium-based)	Exposure of private personal information to an unauthorized actor in Microsoft Edge for Android allows an unauthorized attacker to disclose information over a network.	2026-07-03	7.1	CVE-2026-58296
Microsoft-- Microsoft Edge (Chromium-based)	Exposure of private personal information to an unauthorized actor in Microsoft Edge for Android allows an unauthorized attacker to disclose information over a network.	2026-07-03	7.1	CVE-2026-58297
Microsoft-- Microsoft Edge (Chromium-based)	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-07-03	7.2	CVE-2026-58298
Microsoft-- Microsoft Edge	Time-of-check time-of-use (toctou) race condition in Microsoft Edge for Android allows an unauthorized attacker to execute code over a network.	2026-07-03	7.5	CVE-2026-58299

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
(Chromium-based)				
Microsoft--Microsoft Entra Provisioning Service	Server-side request forgery (ssrf) in Microsoft Entra Provisioning Service (SyncFabric) allows an authorized attacker to elevate privileges over a network.	2026-07-02	9.9	CVE-2026-57100
Microsoft--Microsoft Exchange Online	Incorrect authorization in Microsoft Exchange Online allows an authorized attacker to elevate privileges over a network.	2026-07-02	8.8	CVE-2026-54998
microsoft--OpenAPI.NET	The OpenAPI.NET SDK contains a useful object model for OpenAPI documents in .NET along with common serializers to extract raw OpenAPI JSON and YAML documents from the model. From 2.0.0-preview11 until 2.7.5 and 3.5.4, a small OpenAPI document containing a circular schema reference can cause process termination through stack overflow in Microsoft.OpenApi. The issue affects OpenAPI document parsing through public OpenAPI.NET reader APIs and has been confirmed across both JSON and YAML reader paths. This vulnerability is fixed in 2.7.5 and 3.5.4.	2026-06-30	7.5	CVE-2026-49451
mjperpinosa--stumasy	A vulnerability was identified in mjperpinosa stumasy up to 327d1b0f2915ba79d7ef8ebb74553e987609d9be. Impacted is the function eval of the file application/pages/imba_calculator/calculate.php. The manipulation of the argument mathematical_sentence leads to code injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	2026-07-05	7.3	CVE-2026-14749
mjperpinosa--stumasy	A security flaw has been discovered in mjperpinosa stumasy up to 327d1b0f2915ba79d7ef8ebb74553e987609d9be. The affected element is the function Notes_controller::accessing_dictionary_authorization of the file application/PHP/objects/notes/accessing_dictionary_authorization.php. The manipulation of the argument Password results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	2026-07-05	7.3	CVE-2026-14750
mjperpinosa--stumasy	A vulnerability was detected in mjperpinosa stumasy up to 327d1b0f2915ba79d7ef8ebb74553e987609d9be. This impacts an unknown function of the file /PHP/objects/notes of the component Note Handler/Assignment Handler. Performing a manipulation of the argument assignment_item_id results in authorization bypass. The attack can be initiated remotely. The exploit is now public and may be used. Continuous delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	2026-07-05	7.3	CVE-2026-14753
modoboa--modoboa	Modoboa before 2.9.0 contains an insecure direct object reference vulnerability in the PUT /api/v1/accounts/{pk}/password/ endpoint that allows domain administrators to change any user's password. Attackers with domain admin privileges can bypass object-level access controls to reset superadmin passwords and achieve full account takeover.	2026-06-29	7.5	CVE-2026-56780
Moreconvert Team--MC Woocommerce Wishlist	Unauthenticated Cross Site Scripting (XSS) in MC Woocommerce Wishlist <= 1.9.19 versions.	2026-07-02	7.1	CVE-2026-57356
msgpack--msgpack-python	MessagePack is the serializer implementation for Python msgpack.org. Prior to 1.2.1, there is an Out-of-bounds read/crash on Unpacker reuse	2026-06-30	7.5	CVE-2026-57585

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	after a caught error, potentially leading to a DoS attack. If the Unpacker is used repeatedly after an error occurs, the process may crash with a SEGV. This issue has been fixed in version 1.2.1.			
n8n--n8n	The Execute Command node in n8n allows authenticated users to execute arbitrary commands on the host system where n8n runs. Attackers with user access or compromised credentials can exploit this node to run malicious commands, potentially leading to data exfiltration, service disruption, or complete system compromise.	2026-07-04	8.8	CVE-2025-71380
neuml--txtai	txtai through 9.10.0, fixed in commit 11b32da, exposes an API /reindex endpoint whose function body parameter is resolved through txtai.util.Resolver, which performs __import__ and getattr on the caller-supplied dotted path with no allowlist. When the API is exposed with no TOKEN configured (authentication is opt-in, so all endpoints are unauthenticated) and the index is configured writable, a remote attacker can set function to an arbitrary callable such as subprocess.getoutput, achieving remote code execution as the server process during reindexing. Exploitation requires those deployment conditions (API exposed, no TOKEN, writable index); it is not the default configuration. The fix gates the endpoint behind a new reindex configuration flag.	2026-06-30	9.8	CVE-2026-58449
NodeBB--NodeBB	NodeBB does not bind the claimed author of an inbound ActivityPub object to the authenticated remote actor. The inbound middleware verifies the HTTP-signature actor and checks the origin of object.id, but never validates that attributedTo corresponds to the sender. In the object mock, attributedTo is used directly as a uid, and actors.assert silently ignores numeric identifiers (filtering them out without re-deriving the uid), so a federated remote actor can set attributedTo to a bare numeric value such as 1 and have the resulting post or private message created with that local uid as author, including the administrator account. This lets a remote attacker forge posts and direct messages attributed to arbitrary local users. Requires the ActivityPub/federation feature to be enabled.	2026-07-01	7.5	CVE-2026-58593
Notifiarr--dockwatch	Dockwatch through 0.6.567 contains an unauthenticated OS command injection vulnerability that allows remote attackers to execute arbitrary shell commands by exploiting a missing exit() after an authentication redirect in loader.php combined with unsanitized input passed to shell_exec() in ajax/compose.php. Attackers can seed the required session flag through the incomplete auth check, then inject arbitrary commands via the composePath POST parameter in the composePull action to achieve full host compromise, facilitated by the standard deployment mounting of the Docker socket.	2026-07-02	9.8	CVE-2026-58455
Novalnet--Novalnet Payment Gateway for WooCommerce	Unauthenticated PHP Object Injection in Novalnet Payment Gateway for WooCommerce <= 12.10.3 versions.	2026-07-02	9.8	CVE-2026-57677
NVIDIA--AIStore framework	NVIDIA AIStore framework contains a vulnerability where an attacker could bypass authentication. A successful exploit of this vulnerability might lead to denial of service, escalation of privileges, information disclosure, and data tampering.	2026-07-01	9.8	CVE-2026-24270
NVIDIA--BlueField GA	NVIDIA ConnectX and BlueField contain a vulnerability in the command interface where a local user with virtual function (VF) access may cause a write out of bounds by crafted input. A successful exploit of this vulnerability may lead to arbitrary code execution on the device.	2026-07-01	9	CVE-2025-23350
NVIDIA--BlueField GA	NVIDIA ConnectX and BlueField contain a vulnerability in the command interface where a local user with virtual function (VF) access may cause a write out of bounds by crafted input. A successful exploit of this vulnerability may lead to arbitrary code execution on the device.	2026-07-01	9	CVE-2025-23351
NVIDIA--Container Toolkit	NVIDIA Container Toolkit for Linux contains a vulnerability where an attacker could cause a time-of-check time-of-use race condition. A	2026-07-01	8.5	CVE-2026-24260

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	successful exploit of this vulnerability might lead to code execution, escalation of privileges, and data tampering.			
NVIDIA--Megatron-Bridge	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	2026-07-01	7.8	CVE-2026-24240
NVIDIA--Megatron-Bridge	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause server-side request forgery. A successful exploit of this vulnerability might lead to information disclosure.	2026-07-01	7.8	CVE-2026-24242
NVIDIA--Megatron-Bridge	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	2026-07-01	7.8	CVE-2026-24243
NVIDIA--Megatron-Bridge	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	2026-07-01	7.8	CVE-2026-24244
NVIDIA--Megatron-Bridge	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	2026-07-01	7.8	CVE-2026-24245
NVIDIA--Megatron-Bridge	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause improper control of dynamically managed code resources. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	2026-07-01	7.8	CVE-2026-24246
NVIDIA--Megatron-Bridge	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	2026-07-01	7.8	CVE-2026-24247
NVIDIA--Megatron-Bridge	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause improper control of code generation. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	2026-07-01	7.8	CVE-2026-24248
NVIDIA--Megatron-Bridge	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause deserialization of untrusted data. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	2026-07-01	7.8	CVE-2026-24249
NVIDIA--Megatron-Bridge	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause improper validation of allowed inputs. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	2026-07-01	7.8	CVE-2026-24250
NVIDIA--Megatron-Bridge	NVIDIA Megatron Bridge for Linux contains a vulnerability where an attacker could cause improper control of dynamically managed code resources. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, and information disclosure.	2026-07-01	7.8	CVE-2026-24251
NVIDIA--Triton Inference Server	NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker can cause improper handling of highly compressed data. A successful exploit of this vulnerability might lead to denial of service.	2026-07-01	7.5	CVE-2026-24264
OFFIS DICOM--DCMTK Toolkit	A malicious or compromised server can make a DCMTK client using bit-preserving C-GET storage mode write files outside the chosen output directory, using both relative (../) paths and absolute paths.	2026-06-30	9.8	CVE-2026-50003
OFFIS DICOM--DCMTK Toolkit	An unauthenticated attacker can read worklist records from a directory outside the intended per-AE worklist storage area. In a multi-area deployment, this can cross departmental or clinic data separation.	2026-06-30	8.2	CVE-2026-52868
OFFIS DICOM--DCMTK Toolkit	An unauthenticated remote attacker can repeatedly send crafted connection requests to leak memory. In single-process deployments the	2026-06-30	7.5	CVE-2026-35505

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	memory grows until the service is killed and the port stops responding until restart.			
OFFIS DICOM--DCMTK Toolkit	An unauthenticated attacker can crash the worklist server with a single crafted query when the server has a valid Called AE Title / storage directory, the expected lockfile, and at least one matching worklist record.	2026-06-30	7.5	CVE-2026-44628
OFFIS DICOM--DCMTK Toolkit	An unauthenticated remote attacker can repeatedly send a single crafted connection request to leak memory. Against storescp in its default single-process mode, memory grows quickly and the service is eventually killed, after which it stops accepting connections until an operator restarts it.	2026-06-30	7.5	CVE-2026-50254
ohler55--oj	Oj (Optimized JSON) is a JSON parser and Object marshaller packaged as a Ruby gem. In versions prior to 3.17.3, Oj::Doc#each_child, when invoked recursively over a deeply nested JSON document, overflows a fixed-size stack buffer and aborts the process, leading to DoS. In a two-step chain in ext/oj/fast.c, doc_each_child increments doc->where past the where_path[MAX_STACK = 100] array with no bounds check and never restores it (the doc->where-- is missing), so calling each_child recursively from inside the yield block drives doc->where beyond the array. On the next entry the function copies the path into the 800-byte stack-local buffer save_path[MAX_STACK] using wlen = doc->where - doc->where_path, so when the previous recursive call left doc->where past where_path[100] the wlen exceeds MAX_STACK and the memcpy overflows save_path on the C stack; because the Oj::Doc parser imposes no JSON nesting-depth limit (relying on a C-stack pressure check), deeply nested attacker input reaches this path. This issue has been fixed in version 3.17.3.	2026-06-30	7.5	CVE-2026-54592
open62541 project / o6 Automation GmbH--open62541	An unauthenticated remote attacker can exhaust server memory via the GetEndpoints Discovery Service in open62541. The endpointUrl field of GetEndpointsRequest is not validated for length. An attacker can declare an arbitrarily large string (up to ~4.09 GB via the UInt32 length field) delivered across intermediate chunks without ever sending the final chunk. The server buffers all chunks in RAM indefinitely until the SecureChannel times out. The attack is pre-session and bypasses all encryption configurations. The issue affects open62541: from 1.4.0 through 1.4.16, from 1.5.0 through 1.5.4, master.	2026-07-02	7.5	CVE-2026-11946
open62541 project / o6 Automation GmbH--open62541	An unauthenticated remote attacker can exhaust server memory via the FindServers Discovery Service in open62541. The serverUri field of FindServersRequest is not validated for length or array size. An attacker can declare an arbitrarily large string (up to ~3.9 GB) delivered across intermediate chunks without ever sending the final chunk. The server buffers all chunks in RAM indefinitely until the SecureChannel times out. The attack is pre-session and bypasses all encryption configuration. The issue affects open62541: from 1.4.0 through 1.4.16, from 1.5.0 through 1.5.4, master.	2026-07-02	7.5	CVE-2026-33592
OpenBMB--ChatDev	OpenBMB ChatDev through 2.2.0, fixed in commit 4fd4da6, contains a path traversal vulnerability that allows unauthenticated remote attackers to write or delete arbitrary files by supplying a malicious multipart filename in the file upload endpoint. Attackers can send a crafted filename containing path traversal sequences or an absolute path to the POST uploads session endpoint, which constructs the destination path without sanitization in save_upload_file, causing file write and cleanup operations to target attacker-chosen paths on the server filesystem.	2026-06-30	9.1	CVE-2026-58166
openSUSE--buildservice	A shellcode injection in the mercurial handler of the obs tar_scm source service before version 0.12.4 could be used by attackers able to provide a _service file to execute code as the source service or the local user checking out the malicious services	2026-07-02	10	CVE-2026-56004
openwrt--luci-app-tailscale-community	luci-app-tailscale-community contains a command injection vulnerability in the tailscale.do_login RPC method that allows authenticated users to execute arbitrary commands as root. The vulnerability exists because user-controlled loginserver and loginserver_authkey parameters are improperly quoted within a double-quoted shell command, allowing shell	2026-06-29	8.8	CVE-2026-57999

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	substitutions like \$() to be evaluated by the outer shell before argument processing.			
openwrt--luci-app-travelmate	luci-app-travelmate (and the travelmate package) contain a privilege-escalation flaw: a LuCI/rpcd session holding the luci-app-travelmate write ACL is granted config-wide UCI write access to the travelmate configuration. While the LuCI UI restricts the auto-login script picker to /etc/travelmate/*.login, this is only a frontend restriction. The backend travelmate service (running as root) reads the raw UCI 'script' and 'script_args' values and executes the configured path when the captive-portal auto-login branch (f_check() in travelmate-functions.sh) is reached. An attacker with delegated write permissions can set script to /bin/sh and script_args to attacker-controlled arguments, resulting in arbitrary command execution as root. Confirmed in luci-app-travelmate/travelmate 2.4.5-r3; the sink is still present in travelmate 2.4.6-1 and no patched version is known.	2026-07-02	7.5	CVE-2026-58652
openwrt--luci-proto-openvpn	luci-proto-openvpn through 0.11.1, fixed in commit e4ff45e, contains a command injection vulnerability in the generateKey ubus method where the cl_meta parameter is interpolated into a shell command without proper escaping or quoting. An authenticated LuCI user with OpenVPN protocol configuration access can inject arbitrary shell metacharacters into cl_meta to execute commands as root via the popen function.	2026-06-29	8.8	CVE-2026-58000
openziti--ziti	OpenZiti through 2.0.0, fixed in commit 3027fdf, contains a privilege escalation vulnerability that allows authenticated non-admin identities with fine-grained enrollment management permissions to create enrollments for any identity, including the default administrator, because the ApplyCreate function in controller/model/enrollment_manager.go verifies only that the target identity exists without performing authorization checks binding the caller to the target identity. Attackers can redeem the resulting one-time token through the unauthenticated client API enrollment endpoint to obtain a client certificate authenticating as the targeted admin identity, yielding full administrative control of the controller and the zero-trust overlay it manages.	2026-06-30	8.8	CVE-2026-58165
OPPO--O+ Connect	Because O+ Connect's IPC service does not authenticate clients, external applications can escalate privileges and perform sensitive actions through the IPC channel.	2026-06-29	7.3	CVE-2026-22078
Optimole--Optimole	Unauthenticated Cross Site Scripting (XSS) in Optimole <= 4.2.7 versions.	2026-07-02	7.1	CVE-2026-57673
pathwaycom--pathway	Pathway through 0.31.1, fixed in commit d09722e, document store applies a caller-supplied glob pattern to indexed document paths using a hand-written recursive matcher that branches two ways on each ** token without memoization, giving exponential worst-case complexity. The filepath_globpattern value is taken from the body of the unauthenticated HTTP endpoints /v1/retrieve, /v1/inputs and /v2/answer and compiled into a filter evaluated once per indexed document, with no length or ** count limit. A remote unauthenticated attacker can submit a short pattern containing many ** tokens to consume CPU for tens of seconds per request, and a small number of requests denies service.	2026-07-02	7.5	CVE-2026-59094
Perfmatters--perfmatters	Unauthenticated Cross Site Scripting (XSS) in perfmatters <= 2.6.4 versions.	2026-07-02	7.1	CVE-2026-57671
perfmatters--Perfmatters	The Perfmatters plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 2.6.4 via the 's' parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. Exploitation requires the Local Google Fonts feature to be enabled (disabled by default), pretty permalinks to be active, and RSS feed links to remain enabled in the plugin settings.	2026-07-02	7.5	CVE-2026-13251
pfefferle--Webmention	The Webmention plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to and including 5.8.0 via parser-derived 'avatar' and 'url' author metadata. This is due to insufficient input sanitization and	2026-06-30	7.2	CVE-2026-10513

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	output escaping on user-supplied MF2 author properties processed by the unauthenticated webmention REST endpoint and rendered directly into HTML 'value' attributes by the edit-comment-form template without esc_attr() or esc_url(). This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a privileged user (moderator or administrator) opens the affected comment edit screen.			
phpMyFAQ-- phpMyFAQ	phpMyFAQ before 4.1.5 contains a privilege escalation vulnerability in GroupController::updatePermissions that allows GROUP_EDIT administrators to grant arbitrary rights to groups without verifying they hold those rights themselves. A delegated administrator can exploit this by assigning high-value permissions to a group they belong to, inheriting those rights and escalating privileges up to full administrative control.	2026-06-30	8.8	CVE-2026-57995
Picklescan-- Picklescan	Picklescan before 0.0.33 fails to detect the numpy.f2py.crackfortran.getlincoef gadget in pickle __reduce__ methods, allowing arbitrary code execution. Attackers can craft malicious pickle files that execute arbitrary Python code when loaded, bypassing Picklescan's safety checks and enabling supply-chain poisoning of shared model files.	2026-07-04	8.1	CVE-2025-71372
picklescan-- picklescan	picklescan before 0.0.30 fails to detect malicious pickle files using idlelib.run.Executive.runcode in reduce methods. Attackers can embed undetected code in pickle files that executes during pickle.load, enabling remote code execution in PyTorch models and supply chain attacks.	2026-07-04	8.1	CVE-2025-71342
picklescan-- picklescan	picklescan before 0.0.30 fails to detect malicious pickle files that exploit lib2to3.pgen2.pgen.ParserGenerator.make_label function in the reduce method. Attackers can craft malicious pickle files with embedded code that evades detection but executes arbitrary commands when pickle.load() is called.	2026-07-04	8.1	CVE-2025-71343
picklescan-- picklescan	picklescan before 0.0.30 fails to detect malicious pickle files that invoke torch.utils.bottleneck.__main__.run_autograd_prof function. Attackers can embed undetected code in pickle files that executes during deserialization, enabling remote code execution.	2026-07-04	8.1	CVE-2025-71345
picklescan-- picklescan	picklescan before 0.0.33 fails to detect malicious pickle files using numpy.f2py.crackfortran.param_eval function in reduce methods, allowing attackers to bypass security checks. Remote attackers can embed undetected code in pickle files that executes during deserialization, enabling arbitrary code execution in applications loading untrusted pickle data.	2026-07-04	8.1	CVE-2025-71347
picklescan-- picklescan	picklescan before 0.0.29 fails to detect the built-in trace.Trace.run function when analyzing pickle files, allowing attackers to embed undetected malicious code. Remote attackers can craft malicious pickle files using trace.Trace.run in the reduce method to achieve arbitrary code execution when pickle.load processes the file.	2026-06-30	8.1	CVE-2025-71349
picklescan-- picklescan	picklescan before 0.0.28 fails to detect malicious pickle files using torch.utils.collect_env.run function in reduce methods. Attackers can embed undetected code in pickle files that executes remote commands when loaded by victims.	2026-06-30	8.1	CVE-2025-71350
picklescan-- picklescan	picklescan before 0.0.29 fails to detect the built-in Python trace.Trace.runtctx function when used in pickle file reduce methods, allowing attackers to execute arbitrary code. Remote attackers can craft malicious pickle files with trace.Trace.runtctx payloads that bypass picklescan detection and execute code upon pickle.load() invocation.	2026-06-30	8.1	CVE-2025-71352
picklescan-- picklescan	picklescan before 0.0.28 fails to detect malicious pickle files that exploit torch._dynamo.guards.GuardBuilder.get function in reduce methods. Attackers can craft pickle files with embedded code that evades picklescan detection and executes arbitrary commands when loaded.	2026-07-04	8.1	CVE-2025-71353
picklescan-- picklescan	picklescan before 0.0.28 fails to detect malicious torch.fx.experimental.symbolic_shapes.ShapeEnv.evaluate_guards_expression function calls in pickle files. Attackers can embed undetected code in pickle files that executes remote code when loaded by victims.	2026-07-04	8.1	CVE-2025-71356

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
picklescan--picklescan	picklescan before 0.0.29 fails to detect malicious pickle payloads that utilize lib2to3.pgen2.grammar.Grammar.loads in the reduce method, allowing remote code execution. Attackers can craft pickle files embedding dangerous code that evades picklescan detection and executes during pickle.load() deserialization.	2026-07-04	8.1	CVE-2025-71359
picklescan--picklescan	picklescan before 0.0.29 fails to detect malicious pickle files using idlelib.calltip.get_entity function in reduce methods. Attackers can embed undetected code in pickle files that executes remote commands when loaded by victims.	2026-07-04	8.1	CVE-2025-71360
picklescan--picklescan	picklescan before 0.0.33 fails to detect unsafe deserialization when numpy.f2py.crackfortran functions call eval on arbitrary strings. Attackers can embed malicious code in pickle files that executes when loaded from untrusted sources.	2026-07-04	8.1	CVE-2025-71362
picklescan--picklescan	picklescan before 0.0.30 fails to detect cProfile.run function calls in pickle reduce methods, allowing attackers to execute arbitrary code. Remote attackers can craft malicious pickle files with cProfile.run payloads that bypass picklescan detection and achieve code execution upon deserialization.	2026-06-30	8.1	CVE-2025-71363
picklescan--picklescan	picklescan before 0.0.30 fails to detect the asyncio.unix_events._UnixSubprocessTransport._start function in pickle reduce methods, allowing remote code execution. Attackers can craft malicious pickle files embedding this built-in function that evade detection but execute arbitrary commands when loaded.	2026-07-04	8.1	CVE-2025-71364
picklescan--picklescan	picklescan before 0.0.28 fails to detect malicious torch.utils.bottleneck.__main__.run_cprofile function calls in pickle files, allowing attackers to bypass safety checks. Remote attackers can embed undetected code in pickle files to achieve arbitrary code execution when victims load the files.	2026-07-04	8.1	CVE-2025-71366
picklescan--picklescan	picklescan before 0.0.34 fails to detect _operator.attrgetter function calls in pickle payloads, allowing attackers to bypass security checks. Remote attackers can craft malicious pickle files using _operator.attrgetter in reduce methods to execute arbitrary code when pickle.load() processes the file.	2026-07-04	8.1	CVE-2025-71367
picklescan--picklescan	picklescan before 0.0.30 fails to detect the doctest.debug_script function when analyzing pickle files, allowing attackers to execute arbitrary code. Remote attackers can craft malicious pickle files embedding doctest.debug_script calls that bypass picklescan detection and execute arbitrary commands upon pickle.load invocation.	2026-06-30	8.1	CVE-2025-71368
picklescan--picklescan	picklescan before 0.0.28 fails to detect malicious pickle files that use torch.utils.data.datapipes.utils.decoder.basichandlers in reduce methods, allowing attackers to bypass safety checks. Remote attackers can embed undetected malicious code in pickle files that executes during deserialization, enabling remote code execution.	2026-07-04	8.1	CVE-2025-71369
picklescan--picklescan	picklescan before 0.0.29 fails to detect malicious pickle files using code.InteractiveInterpreter.runcode in reduce methods. Attackers can craft pickle payloads that bypass picklescan detection and execute arbitrary code when loaded via pickle.load().	2026-06-30	8.1	CVE-2025-71371
picklescan--picklescan	picklescan before 0.0.33 fails to detect operator.methodcaller function calls in pickle files, allowing attackers to bypass security checks. Remote attackers can craft malicious pickle payloads using operator.methodcaller that execute arbitrary code when loaded, compromising systems relying on picklescan for validation.	2026-07-04	8.1	CVE-2025-71373
picklescan--picklescan	picklescan before 0.0.29 fails to detect the built-in python profile.Profile.run function when used in pickle reduce methods, allowing attackers to execute arbitrary code. Remote attackers can craft malicious pickle files that bypass picklescan detection and achieve code execution upon deserialization.	2026-06-30	8.1	CVE-2025-71374
picklescan--picklescan	picklescan before 0.0.34 fails to detect the _operator.methodcaller built-in function when scanning pickle files for malicious code. Attackers can craft	2026-07-04	8.1	CVE-2025-71375

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	malicious pickle payloads using <code>_operator.methodcaller</code> that evade detection and execute arbitrary code when loaded by <code>pickle.load()</code> .			
pinpoint-apm--pinpoint	Pinpoint through 3.1.0 contains a server-side request forgery vulnerability in the webhook registration endpoint that allows authenticated users to register internal URLs due to missing SSRF protection. Attackers can trigger alarm threshold breaches to force the server to issue POST requests to internal hosts and metadata endpoints, enabling unauthorized access to internal network resources.	2026-06-29	8.5	CVE-2026-57947
ploudapp--pCloud WP Backup	Unauthenticated Cross Site Request Forgery (CSRF) in pCloud WP Backup <= 2.0.2 versions.	2026-07-02	7.1	CVE-2026-57757
PluginOps--Landing Page Builder	Unauthenticated Cross Site Scripting (XSS) in Landing Page Builder <= 1.5.3.5 versions.	2026-06-29	7.1	CVE-2026-57337
printcart--Printcart Web to Print Product Designer for WooCommerce	The Printcart Web to Print Product Designer for WooCommerce plugin for WordPress is vulnerable to Arbitrary File Deletion in versions up to, and including, 2.5.2 This is due to insufficient path validation in the <code>store_design_data()</code> function, which constructs a filesystem path from the user-supplied 'nbd_item_key' POST parameter sanitized only with <code>sanitize_text_field()</code> - which does not strip path traversal sequences - and then passes that path directly to <code>Nbdesigner_IO::delete_folder()</code> and PHP's <code>rename()</code> . The nonce protecting the <code>nbd_save_customer_design</code> AJAX action is freely obtainable by unauthenticated users via the <code>nbd_check_use_logged_in</code> endpoint. This makes it possible for unauthenticated attackers to delete arbitrary files on the affected site's server which may make remote code execution possible.	2026-07-03	9.1	CVE-2026-9725
qlstudio--Export User Data	The Export User Data plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the <code>unserialize</code> function in all versions up to, and including, 2.2.6. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as <code>wp-config.php</code>). Successful exploitation requires an administrator to trigger a user data export while a subscriber-level (or higher) user has stored a crafted serialized <code>XLWXWriter</code> object payload as their display name.	2026-06-30	8	CVE-2026-12240
QuantumCloud--ChatBot	Unauthenticated Cross Site Scripting (XSS) in ChatBot <= 8.3.2 versions.	2026-07-02	7.1	CVE-2026-57362
QuantumCloud--Simple Link Directory	Unauthenticated Cross Site Scripting (XSS) in Simple Link Directory <= 15.0.5 versions.	2026-07-02	7.1	CVE-2026-57682
quantumcloud--WPBot AI ChatBot for Live Support, Lead Generation, AI Services	The WPBot - AI ChatBot for Live Support, Lead Generation, AI Services plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'conversation' parameter in all versions up to, and including, 8.4.9 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The AJAX nonce required to authenticate the save request is publicly emitted on every frontend page via <code>wp_localize_script</code> , making it freely obtainable by any anonymous visitor and removing any practical barrier to exploitation.	2026-07-01	7.2	CVE-2026-13731
RadiusTheme--Classified Listing	Unauthenticated Cross Site Scripting (XSS) in Classified Listing <= 5.4.2 versions.	2026-07-02	7.1	CVE-2026-57344
Raera - Ankara Web Design and Digital Advertising Agency--Destekz	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in Raera - Ankara Web Design and Digital Advertising Agency Destekz allows SQL Injection. This issue affects Destekz: through 02062026. NOTE: The vendor was contacted and it was learned that the product is not supported.	2026-07-03	9.8	CVE-2026-4321
RARLAB--WinRAR	An out-of-bounds heap write exists in the RAR5 recovery-volume (.rev) parser in WinRAR and UnRAR (<code>RecVolumes5::ReadHeader</code> in <code>revol5.cpp</code>). The <code>Recltems</code> vector is sized only when the first .rev file in a set is	2026-07-01	7.8	CVE-2026-14191

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	processed; subsequent .rev files supply an independent RecNum value that is validated against that file's own TotalCount field but never against the actual size of RecItems. A crafted set of two or more .rev files can therefore write an attacker-controlled 32-bit value (the header's RevCRC field) to RecItems[RecNum] at an attacker-controlled offset up to 65534 * sizeof(RecVolltem) bytes past the allocation, corrupting adjacent heap objects. Triggering requires the victim to run a recovery/test operation on an attacker-supplied .rev set (for example 'unrar t x.part1.rev', WinRAR 'Repair archive', or auto-recovery when extracting a volume set with a missing .rar part). This is the RAR5-path sibling of CVE-2023-40477 (which was fixed in the RAR3 path only in WinRAR 6.23). Fixed in WinRAR / RAR 7.23.			
RealMag777--BEAR	Unauthenticated Cross Site Scripting (XSS) in BEAR <= 1.1.8 versions.	2026-06-29	7.1	CVE-2026-57320
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in HPLIP (HP Linux Imaging and Printing Software). This vulnerability, an incomplete fix for CVE-2026-8631, may allow a remote attacker to escalate privileges or achieve arbitrary code execution. This can occur through an integer overflow in the hpcups processing path when handling specially crafted print data.	2026-07-03	9.8	CVE-2026-14544
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in Yelp due to an overly permissive Content Security Policy (CSP) implementation provided by yelp-xsl. A malicious Flatpak application can open crafted help content through the OpenURI portal. By embedding an untrusted CSS stylesheet within a structured SVG document, attacker-controlled content can bypass Flatpak's intended sandbox isolation, allowing Yelp to evaluate local XML inclusions and disclose arbitrary user-readable host files through remote CSS resource requests. This may result in the unauthorized disclosure of sensitive information.	2026-06-29	7.1	CVE-2026-13601
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in GIMP's Paint Shop Pro (PSP) file format parser. This heap buffer overflow vulnerability allows a remote attacker to cause arbitrary code execution or a denial of service (DoS) by tricking a user into opening a specially crafted PSP image file. The vulnerability occurs because the software incorrectly calculates buffer sizes when processing low bit-depth images, leading to an overwrite of adjacent memory.	2026-07-03	7.3	CVE-2026-58379
Red Hat--Red Hat Hardened Images	A flaw was found in libtiff. A remote attacker could exploit this vulnerability by providing a specially crafted PixarLog-compressed TIFF image. This issue occurs when decoding Pixarlog codec images with the PIXARLOGDATAFMT_8BITABGR output format and a specific stride value, leading to a heap-based buffer overflow. This could potentially result in arbitrary code execution or a denial of service (DoS).	2026-06-29	7.3	CVE-2026-12912
Red Hat--Red Hat Hardened Images	A double free issue has been identified in libarchive's RAR5 reader. During parsing of a specially crafted RAR5 archive, the filtered_buf pointer may remain stale after being freed during unpacking state reinitialization. Subsequent processing of another archive entry can trigger a second free of the same memory region, resulting in a double-free condition. Successful exploitation may cause applications using the vulnerable libarchive API to terminate unexpectedly, leading to a denial of service.	2026-06-30	7.5	CVE-2026-14164
Red Hat--Red Hat OpenShift Dev Spaces	A flaw was found in the vscode-java extension, which provides Java language support for Visual Studio Code. The extension incorrectly trusts all Markdown content in JavaDoc hovers, allowing a malicious Java file to include hidden commands. If a user clicks a specially crafted link within a JavaDoc hover popup, an attacker can execute arbitrary VS Code commands, which can lead to full system compromise in trusted workspaces.	2026-06-29	8.8	CVE-2026-12856
Red Hat--Red Hat Satellite 6.16 for RHEL 8	A flaw was found in Foreman. The Usergroup model in Foreman does not properly validate role assignments against the calling user's permissions. This allows an authenticated user with usergroup management permissions to attach arbitrary roles, including administrative roles, to a user group and then add themselves as a member. Successful exploitation	2026-07-01	8.8	CVE-2026-5136

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of this vulnerability leads to full privilege escalation, granting the attacker administrator-level access.			
Repute InfoSystems--ARForms	Unauthenticated Cross Site Scripting (XSS) in ARForms <= 7.1.2 versions.	2026-06-29	7.1	CVE-2026-57338
Repute Infosystems--BookingPress Appointment Booking Pro	The BookingPress Appointment Booking Pro plugin for WordPress is vulnerable to SQL Injection via the 'store_service_date' parameter of the bpa_assign_staffmember_to_slots() function in versions up to and including 5.7.1. This is due to the explicit use of stripslashes_deep() on user-supplied POST data before it is interpolated verbatim into a SQL LIKE clause without use of \$wpdb->prepare() or any parameterization. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-07-01	7.5	CVE-2026-11823
Reputeinfosystems--ARMember Premium	Contributor PHP Object Injection in ARMember Premium <= 7.0 versions.	2026-07-02	8.8	CVE-2026-27060
ReviewX--ReviewX	Unauthenticated Cross Site Scripting (XSS) in ReviewX <= 2.3.10 versions.	2026-07-02	7.1	CVE-2026-57359
RT-Thread--RT-Thread	A vulnerability was identified in RT-Thread up to 5.0.2. Affected by this vulnerability is the function recvmmsg in the library bsp/loongson/ls1cdev/libraries/ls1c_can.h of the component ls1c CAN Handler. Such manipulation leads to stack-based buffer overflow. Local access is required to approach this attack. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-07-03	7.8	CVE-2026-14605
RT-Thread--RT-Thread	A security flaw has been discovered in RT-Thread up to 5.0.2. Affected by this issue is the function CAN_Receive in the library bsp/synwit/libraries/SWM341_CSL/CMSIS/DeviceSupport/SWM341.h of the component SWM341 CAN Handler. Performing a manipulation results in stack-based buffer overflow. The attack needs to be approached locally. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-07-03	7.8	CVE-2026-14606
Ruijie--RG-UAC	A vulnerability was found in Ruijie RG-UAC up to 1.0-R1.8.2.p5. The impacted element is an unknown function of the file user_auth_commit.php. Performing a manipulation of the argument upload_image results in unrestricted upload. The attack is possible to be carried out remotely. The exploit has been made public and could be used.	2026-07-05	7.3	CVE-2026-14736
Rustaurius--Five Star Business Profile and Schema	Editor Arbitrary Code Execution in Five Star Business Profile and Schema <= 2.3.19 versions.	2026-07-02	9.1	CVE-2026-27436
SaturdayDrive--Ninja Forms - File Uploads	The Ninja Forms - File Uploads plugin for WordPress is vulnerable to Arbitrary File Read via the attach_files() function in versions up to, and including, 3.3.29. This is due to the get_files_for_attachment() function accepting a raw attacker-controlled 'files' array when the process() method returns early due to a client-supplied saveProgress flag, bypassing all upload validation, path normalization, and database record creation steps, and allowing an attacker-supplied file_path value to reach wp_mail() as an email attachment with only a file_exists() check. This makes it possible for unauthenticated attackers to read arbitrary files on the affected site's server.	2026-07-02	7.5	CVE-2026-13369
Search Atlas Group--Search Atlas SEO	Unauthenticated Cross Site Scripting (XSS) in Search Atlas SEO <= 2.6.6 versions.	2026-07-02	7.1	CVE-2026-57357
seaweedfs--seaweedfs	SeaweedFS before 4.34 contains a path traversal vulnerability in the S3 gateway DeleteMultipleObjectsHandler that allows authenticated S3 principals with write access to a single bucket to delete arbitrary objects in	2026-06-30	8.1	CVE-2026-58372

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	other tenants' buckets by supplying object keys containing ../ sequences in the DeleteObjects XML request body. Attackers can bypass authorization controls through a confused deputy condition, as the validateRequestPath middleware only inspects URL-captured path variables and never examines request-body keys, allowing the filer path to collapse directory traversal sequences and resolve deletions outside the authorized bucket.			
Shenzhen Aitemi E Commerce Co. Ltd.--M300 Wi-Fi Repeater	Shenzhen Aitemi M300 Wi-Fi Repeater (hardware model MT02) contains an unauthenticated OS command injection vulnerability that allows network-adjacent attackers to execute arbitrary shell commands by injecting unsanitized input through the smacfilter_conf handler in the commuos web backend. Attackers can append semicolon-delimited payloads to the name, enable, or mac GET parameters, which are passed without sanitization into sprintf() to build uci shell commands executed via doSystemCmdComlib(), granting full root-level control of the device.	2026-07-01	9.8	CVE-2026-58457
Shenzhen Landray Software Co., Ltd.--Landry Office Automation (OA)	Landray OA contains an unauthenticated HQL injection vulnerability that allows unauthenticated attackers to query arbitrary Hibernate entity classes by injecting malicious HQL syntax into the uid POST parameter of the wechatLoginHelper.do endpoint. Attackers can exploit the lack of input sanitization in the string-concatenated filter expression passed to the Hibernate findList() call to extract sensitive data such as administrator password hashes and, with sufficient database privileges, perform file-write operations enabling remote code execution. Exploitation evidence was first observed by the Shadowserver Foundation on 2024-03-11 (UTC).	2026-07-02	7.5	CVE-2024-58352
shimosyan--phpUploader	phpUploader before 2.0.2 contains an unauthenticated information disclosure vulnerability that allows remote attackers to access the full contents of the uploaded-files database table by visiting any page of the application. The index model executes an unbounded SELECT query and embeds the complete JSON-encoded result set in an inline script block, exposing uploader IP addresses, Argon2ID key hashes, internal filenames, and SHA-256 fingerprints.	2026-06-29	7.5	CVE-2026-56124
Shopify Help Center--Shopify	Contributor Local File Inclusion in Shopify <= 1.0.0 versions.	2026-07-02	7.5	CVE-2026-57748
SigNoz--signoz	SigNoz through 0.130.1 contains a SQL injection vulnerability that allows authenticated attackers to execute arbitrary ClickHouse queries by injecting URL-encoded quotes into the rule ID path parameter of the alert-history endpoints. Attackers can manipulate the unsanitized rule ID interpolated into ClickHouse queries to read all stored traces, logs, and metrics, or abuse the url() function to perform server-side request forgery.	2026-06-29	8.5	CVE-2026-57955
Snowflake--Snowflake CLI	Improper neutralization of attacker-controlled content in Snowflake CLI versions prior to 3.19 allowed unintended SQL execution. By supplying crafted repository content, project configuration, manifest data, or specification input, an attacker could cause Snowflake CLI to execute unintended SQL in the context of the victim user's Snowflake session. Successful exploitation requires the victim to process attacker-controlled content through a vulnerable command path and is limited by the privileges assigned to that session. The fix is available in Snowflake CLI version 3.19. Users must manually upgrade.	2026-06-29	8.3	CVE-2026-13744
Snowflake--Snowflake CLI	Improper neutralization in the Snowpark annotation processor callback template in Snowflake CLI versions prior to 3.19 allowed arbitrary code execution during application bundling or deployment. An attacker could exploit this by supplying crafted project content that is interpolated into generated Python code, causing Snowflake CLI to execute attacker-controlled code in the local context of the user running the CLI. Successful exploitation requires the victim to run the relevant bundling or deployment workflow against attacker-controlled project content, and any resulting code runs with the privileges of that local execution context. The fix is available in Snowflake CLI version 3.19, and users must manually upgrade.	2026-06-29	8.8	CVE-2026-13749

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SourceCodester--Class and Exam Timetabling System	A vulnerability was identified in SourceCodester Class and Exam Timetabling System 1.0/5.php. Affected by this vulnerability is an unknown functionality of the file /preview5.php. Such manipulation of the argument course_year_section leads to sql injection. The attack may be performed from remote. The exploit is publicly available and might be used.	2026-06-29	7.3	CVE-2026-13521
SourceCodester--Class and Exam Timetabling System	A flaw has been found in SourceCodester Class and Exam Timetabling System 1.0. Impacted is an unknown function of the file /edit_class.php. This manipulation of the argument ID causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	2026-06-29	7.3	CVE-2026-13526
SourceCodester--Class and Exam Timetabling System	A vulnerability has been found in SourceCodester Class and Exam Timetabling System 1.0. The affected element is an unknown function of the file /preview4.php. Such manipulation of the argument course_year_section leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2026-06-29	7.3	CVE-2026-13527
SourceCodester--Class and Exam Timetabling System	A vulnerability was determined in SourceCodester Class and Exam Timetabling System 1.0/1.php. Affected by this vulnerability is an unknown functionality of the file /edit_class1.php. Executing a manipulation of the argument ID can lead to sql injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized.	2026-06-29	7.3	CVE-2026-13565
SourceCodester--Class and Exam Timetabling System	A vulnerability was identified in SourceCodester Class and Exam Timetabling System 1.0. Affected by this issue is some unknown functionality of the file /preview3.php. The manipulation of the argument course_year_section leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	2026-06-29	7.3	CVE-2026-13566
SourceCodester--Class and Exam Timetabling System	A vulnerability was determined in SourceCodester Class and Exam Timetabling System 1.0. Affected by this vulnerability is an unknown functionality of the file /edit_course.php. Executing a manipulation of the argument ID can lead to sql injection. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized.	2026-07-04	7.3	CVE-2026-14641
SourceCodester--Class and Exam Timetabling System	A vulnerability was identified in SourceCodester Class and Exam Timetabling System 1.0. Affected by this issue is some unknown functionality of the file /edit_class2.php. The manipulation of the argument ID leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	2026-07-04	7.3	CVE-2026-14642
SourceCodester--Class and Exam Timetabling System	A security vulnerability has been detected in SourceCodester Class and Exam Timetabling System 1.0. This vulnerability affects unknown code of the file /edit_exam.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	2026-07-05	7.3	CVE-2026-14732
SourceCodester--Class and Exam Timetabling System	A vulnerability was detected in SourceCodester Class and Exam Timetabling System 1.0. This issue affects some unknown processing of the file /edit_coursea.php. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	2026-07-05	7.3	CVE-2026-14733
SourceCodester--Class and Exam Timetabling System	A flaw has been found in SourceCodester Class and Exam Timetabling System 1.0. Impacted is an unknown function of the file /edit_product.php. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	2026-07-05	7.3	CVE-2026-14734
SourceCodester--Class and Exam Timetabling System	A vulnerability was detected in SourceCodester Class and Exam Timetabling System 1.0. Impacted is an unknown function of the file /edit_room.php. Performing a manipulation of the argument ID results in sql injection. It is possible to initiate the attack remotely. The exploit is now public and may be used.	2026-07-05	7.3	CVE-2026-14770
SourceCodester--Class and Exam Timetabling System	A flaw has been found in SourceCodester Class and Exam Timetabling System 1.0/1.php. The affected element is an unknown function of the file /edit_exam1.php. Executing a manipulation of the argument ID can lead to sql injection. It is possible to launch the attack remotely. The exploit has been published and may be used.	2026-07-05	7.3	CVE-2026-14771

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SourceCodester--Class and Exam Timetabling System	A vulnerability has been found in SourceCodester Class and Exam Timetabling System 1.0/1.php. The impacted element is an unknown function of the file /edit_course1.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2026-07-05	7.3	CVE-2026-14772
SourceCodester--Inventory Management System	A weakness has been identified in SourceCodester Inventory Management System 1.0. This vulnerability affects unknown code of the file /api/users_handler.php of the component User Registration Endpoint. This manipulation of the argument role causes improper access controls. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	2026-06-29	7.3	CVE-2026-13568
SourceCodester--Multi-Vendor Online Grocery Management System	A weakness has been identified in SourceCodester Multi-Vendor Online Grocery Management System 1.0. This affects the function save_users of the file classes/Users.php. This manipulation causes improper authorization. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	2026-07-05	7.3	CVE-2026-14690
SourceCodester--Multi-Vendor Online Grocery Management System	A vulnerability was found in SourceCodester Multi-Vendor Online Grocery Management System 1.0. This affects the function save_client of the file classes/Users.php of the component Registration Handler. The manipulation of the argument Name results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	2026-07-05	7.3	CVE-2026-14695
SourceCodester--Online Examination & Learning Management System	A flaw has been found in SourceCodester Online Examination & Learning Management System 1.0. The impacted element is an unknown function of the file register.php of the component Registration Endpoint. Executing a manipulation of the argument role can lead to improper privilege management. The attack can be executed remotely. The exploit has been published and may be used. The name of the affected product appears to have a typo in it.	2026-07-05	7.3	CVE-2026-14719
SourceCodester--Online Examination & Learning Management System	A security vulnerability has been detected in SourceCodester Online Examination & Learning Management System 1.0. This affects an unknown part of the file /ajax_enroll.php of the component Enrollment Management. The manipulation of the argument student_id/schedule_id/action leads to improper authorization. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The name of the affected product appears to have a typo in it.	2026-07-05	7.3	CVE-2026-14778
SourceCodester--Pizzafy E-Commerce System	A security flaw has been discovered in SourceCodester Pizzafy E-Commerce System 1.0. This vulnerability affects unknown code of the file /admin/ajax.php?action=confirm_order. The manipulation of the argument ID results in sql injection. The attack can be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-07-05	7.3	CVE-2026-14713
SourceCodester--Simple and Nice Shopping Cart Script	A vulnerability was found in SourceCodester Simple and Nice Shopping Cart Script 1.0. This affects an unknown function of the file /admin/login.php of the component Admin Login. The manipulation of the argument Username results in sql injection. The attack may be launched remotely. The exploit has been made public and could be used.	2026-07-04	7.3	CVE-2026-14652
SourceCodester--Simple and Nice Shopping Cart Script	A vulnerability was determined in SourceCodester Simple and Nice Shopping Cart Script 1.0. This impacts an unknown function of the file /admin/mensproductdeletequery.php. This manipulation of the argument user_id causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	2026-07-04	7.3	CVE-2026-14653
SourceCodester--Simple and Nice Shopping Cart Script	A vulnerability was identified in SourceCodester Simple and Nice Shopping Cart Script 1.0. Affected is an unknown function of the file /admin/girlsproductdeletequery.php. Such manipulation of the argument user_id leads to sql injection. The attack can be executed remotely. The exploit is publicly available and might be used.	2026-07-04	7.3	CVE-2026-14654

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Spencer Haws--Link Whisper Free	Unauthenticated Cross Site Scripting (XSS) in Link Whisper Free <= 0.9.4 versions.	2026-06-29	7.1	CVE-2026-57333
StoneFly--Storage Concentrator	Storage Concentrator (SC & SCVM) contains a command injection vulnerability in the ms_service.pl service, which listens on TCP port 9000 by default and accepts custom network packets to perform device actions. An unauthenticated remote attacker can send a specially crafted packet containing a malicious payload that is processed without adequate sanitization, resulting in arbitrary command execution with root-level privileges.	2026-06-30	10	CVE-2026-56413
StoneFly--Storage Concentrator	Storage Concentrator (SC & SCVM) contains hardcoded credentials for numerous internal services embedded within a configuration file. While the credentials are stored in an encoded format, the encoding can be reversed to plaintext. The exposed credentials span a broad range of internal services, including database accounts, licensing, replication services, and third-party integrations, meaning successful exploitation of this vulnerability could provide an attacker with unauthorized access to multiple interconnected systems.	2026-06-30	9.2	CVE-2026-50110
StoneFly--Storage Concentrator	Storage Concentrator (SC & SCVM) is vulnerable to SQL injection through cookie values processed by the login.pl and debug.pl scripts. The cookie value is incorporated directly into database queries without adequate sanitization, allowing an unauthenticated remote attacker to manipulate those queries and extract sensitive information from the underlying database, including session tokens, password hashes, and stored secret keys.	2026-06-30	9.3	CVE-2026-55721
Stonefly--Storage Concentrator	Storage Concentrator (SC & SCVM) contains a command injection vulnerability within the debug.pl script that is reachable without authentication. A remote attacker can submit a specially crafted HTTP request containing a malicious payload that is processed without adequate input sanitization, resulting in arbitrary command execution with root-level privileges on the underlying system.	2026-06-30	10	CVE-2026-56415
StylemixThemes--Pearl - Corporate Business	Unauthenticated Local File Inclusion in Pearl - Corporate Business <= 3.4.10 versions.	2026-07-02	8.1	CVE-2026-27412
SUSE--libzypp	A relative path traversal bug problem when processing repository metadata in libzypp before 17.38.10 could be used by remote attackers supplying repositories to overwrite files on the system, leading to denial of service or privilege escalation.	2026-06-29	8.8	CVE-2026-25707
SUSE--libzypp	A relative path traversal in the "keyhint" option in repomd.xml parsing of libzypp before 17.38.12 can be used by attackers able to supply a malicious repository to inject or overwrite files in the target system as root.	2026-07-02	8.4	CVE-2026-44941
SUSE--Rancher	Missing validation of "valuesFrom" references in Helm Deployer of SUSE Rancher Fleet 0.15 before 0.15.2, 0.14 before 0.14.6, 0.13 before 0.13.11 and 0.12 before 0.12.15 could be used by owners of one tenant to access fleet credentials of other tenants.	2026-07-02	9.9	CVE-2026-44935
SUSE--Rancher	Incorrect authentication caching in the team member ship expansion of the Rancher Github authentication provider caused it granting principal access to any logged in user, in 2.13 before 2.13.6 and 2.14 before 2.14.2.	2026-06-30	8.8	CVE-2026-41053
swaldman--mchange-commons-java	mchange-commons-java is a Java library of shared utility classes used by mchange projects like the c3p0 connection pool. Prior to version 0.6.0, its JNDI ObjectFactory implementation (com.mchange.v2.naming.JaBeanObjectFactory) will construct objects of arbitrary classes and initialize "JaBean"-style properties, which for certain classes enables JNDI injection and "deserialization gadgets." Such initialization is unsafe for some classes: for example, setting the contentType property of a Swing JEditorPane to text/html and its text property to HTML containing a stylesheet <link> will provoke an HTTP GET on an arbitrary URL, potentially from within a trusted security domain. The	2026-07-01	7.1	CVE-2026-55153

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	problem is aggravated by the library's ReferenceIndirector, through which malicious JNDI Reference objects can be smuggled in for dereferencing wherever an application reads a Java-serialized object. This has been resolved in version 0.6.0.			
SysBasics--Customize My Account for WooCommerce	Unauthenticated Cross Site Scripting (XSS) in Customize My Account for WooCommerce <= 4.3.9 versions.	2026-07-02	7.1	CVE-2026-57358
Tenda--JD12L	A flaw has been found in Tenda JD12L 16.03.53.23. The impacted element is the function formWifiBasicSet of the file /goform/WifiBasicSet. Executing a manipulation of the argument security_5g can lead to stack-based buffer overflow. The attack may be launched remotely. The exploit has been published and may be used.	2026-06-29	8.8	CVE-2026-13517
Tenda--JD12L	A vulnerability has been found in Tenda JD12L 16.03.53.23. This affects the function fromAddressNat of the file /goform/addressNat. The manipulation of the argument page leads to stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	2026-06-29	8.8	CVE-2026-13518
Tenda--JD12L	A vulnerability was found in Tenda JD12L 16.03.53.23. This impacts the function fromNatStaticSetting of the file /goform/NatStaticSetting. The manipulation of the argument page results in stack-based buffer overflow. The attack can be executed remotely. The exploit has been made public and could be used.	2026-06-29	8.8	CVE-2026-13519
The Libreswan Project--libreswan	Libreswan, via the function RSA_authenticate_hash_signature_raw_rsa(), did not correctly verify the length of the authentication hash when the SIG payload of an IKEv1 packet was encoded using PKCS #1 RSA Encryption as per RFC 2313. A remote attacker can use a variation on the Bleichenbacher attack to forge the SIG payload when small public exponents are being used (e.g., e=3), which could lead to impersonation. Additionally, a remote attacker, by encoding a shorter than expected hash in the SIG payload, could trigger an assertion leading to denial-of-service. The daemon aborts and restarts; continued exploitation causes sustained denial of service. Remote code execution is not possible. X.509 certificate verifications of remote IKE peers are not affected.	2026-07-02	8.1	CVE-2026-50721
The Libreswan Project--libreswan	Libreswan, via the function RSA_authenticate_hash_signature_pkcs1_1_5_rsa(), did not correctly verify the DER encoding of the ASN.1 digest when the IKEv2 AUTH payload was encoded using RSASSA-PKCS1-v1_5 (RFC 8017). A remote attacker can use a variation on the Bleichenbacher attack to forge the AUTH payload when small public exponents are used (e.g., e=3), leading to impersonation. Additionally, a remote attacker, by encoding a shorter than expected hash in the AUTH payload, could trigger an assertion leading to denial-of-service. The daemon aborts and restarts; continued exploitation causes sustained denial of service. Remote code execution is not possible. X.509 certificate verifications of the remote IKE peer are not affected.	2026-07-02	8.1	CVE-2026-50722
The Libreswan Project--libreswan	An invalidly formatted IKEv2 fragment causes the Libreswan pluto daemon to crash and restart. Continued exploitation would cause a denial of service. The function reassemble_v2_incoming_fragments() would ignore unknown outer payloads but still store these in a fixed size array msg_digest.digest[PAYLIMIT]. An off-by-one error in the assertion PASSERT(logger, md->digest_roof < elemsof(md->digest)) causes the daemon to abort. No remote code execution is possible. Any configuration that allows IKEv2 connections that do not set fragmentation=no are vulnerable. IKEv1 is not affected.	2026-07-02	7.5	CVE-2026-12413
ThemeBoy--SportsPress Pro	Contributor Local File Inclusion in SportsPress Pro <= 2.7.29 versions.	2026-07-02	7.5	CVE-2026-57749
ThemeGoods--Artale Wedding Photography WordPress	Unauthenticated Cross Site Scripting (XSS) in Artale Wedding Photography WordPress <= 2.2.2 versions.	2026-07-02	7.1	CVE-2025-69152

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Photography WordPress				
themeisle-- Visualizer Tables & Charts Manager with Built-in AI Generator	The Visualizer - Tables & Charts Manager with Built-in AI Generator plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.0.3. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to access and export the contents of any visualizer chart on the site - including charts in draft, private, pending, future, or trash status - as CSV, Excel, or HTML via the /wp-json/visualizer/v1/action/{chart}/{type}/ REST endpoint. This bypass is particularly impactful because the standard WordPress REST endpoint for the non-public 'visualizer' custom post type correctly enforces capability checks and returns HTTP 401 to unauthenticated callers, whereas this plugin-registered route circumvents that protection entirely.	2026-07-01	7.5	CVE-2026-13468
ThemeMove-- Unicamp	Subscriber SQL Injection in Unicamp <= 2.2.2 versions.	2026-07-02	8.5	CVE-2025-69094
ThemePunch-- Slider Revolution	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemePunch Slider Revolution allows Reflected XSS. This issue affects Slider Revolution: from 7.0.0 through 7.0.16.	2026-07-02	7.1	CVE-2026-57678
ThemeREX-- Booked	Subscriber Broken Access Control in Booked <= 3.0.0 versions.	2026-07-02	7.1	CVE-2026-57746
Themesuite-- Automotive Car Dealership Business	Unauthenticated Cross Site Scripting (XSS) in Automotive Car Dealership Business <= 13.3.3 versions.	2026-07-02	7.1	CVE-2026-27426
Themesuite-- Automotive Listings	Unauthenticated Cross Site Scripting (XSS) in Automotive Listings <= 18.6 versions.	2026-07-02	7.1	CVE-2026-27425
Themify-- Themify Popup	Deserialization of Untrusted Data vulnerability in Themify Themify Popup allows Object Injection. This issue affects Themify Popup: from n/a through 1.4.3.	2026-07-02	8.8	CVE-2026-56037
ThreeMammals-- Ocelot	Ocelot through 24.1.0, fixed in commit f156fd4, contains a security control bypass vulnerability that allows denied clients to circumvent IP-based access restrictions by sending WebSocket upgrade requests. The WebSocket upgrade pipeline branch configured via MapWhen in OcelotPipelineExtensions.cs omits SecurityMiddleware, causing requests from blocked IP addresses to be proxied to downstream services without enforcement of the configured allow/block list.	2026-06-30	9.1	CVE-2026-58172
tiddly-gittly-- TidGi-Desktop	A vulnerability was found in tiddly-gittly TidGi-Desktop up to 0.13.0. This impacts an unknown function of the file src/services/wiki/wikiWorker/loadWikiTiddlersWithSubWikis.ts of the component Git Repository Import. The manipulation results in code injection. The attack may be performed from remote. The exploit has been made public and could be used.	2026-07-05	7.3	CVE-2026-14722
tinacms-- tinacms	Tina is a headless content management system. @tinacms/cli versions prior to 2.4.3 contain a Remote Code Execution vulnerability in the Forestry-to-Tina migration command. The internal helper addVariablesToCode unquotes any value matching the marker "__TINA_INTERNAL__::(:.*?):::" inside the stringified collection JSON. User-supplied label and name fields from .forestry/**/.yml are placed into that JSON without any sanitisation. An attacker who controls a Forestry-style project can therefore inject arbitrary JavaScript into the generated tina/templates.{ts,js} file. The injected code is written at module top level, so it executes the moment the developer runs tinacms dev or tinacms build, with the developer's privileges. This issue has been fixed in version 2.4.3.	2026-07-01	7.8	CVE-2026-54074
tinypng-- TinyPNG JPEG, PNG & WebP	The TinyPNG - JPEG, PNG & WebP image compression plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_converted_image_size function in all versions	2026-07-02	8.1	CVE-2026-7311

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
image compression	up to, and including, 3.6.13. This makes it possible for authenticated attackers, with author-level access and above, to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php). An attacker can exploit this by injecting an arbitrary server file path into the 'convert.path' field of the 'tiny_compress_images' post meta on an attachment they own, then triggering attachment deletion to invoke the vulnerable code path.			
TR7 Cyber Defense Inc.-- WAF-ASP	Missing authentication for critical function vulnerability in TR7 Cyber -- Defense Inc. WAF-ASP allows Authentication Abuse. This issue affects WAF-ASP: from v1.0.324.900 before v1.4.0.117.	2026-07-02	9.8	CVE-2026-4767
trailofbits--fickling	Trail of Bits fickling versions up to and including 0.1.10 do not include the Python standard library modules _posixsubprocess, site, and atexit in the UNSAFE_IMPORTS denylist (fickle.py). Because these modules are absent from the denylist, fickling's check_safety() function returns LIKELY_SAFE with zero findings for pickle payloads that invoke dangerous functions including _posixsubprocess.fork_exec (C-level process spawner capable of executing arbitrary binaries), site.execsitecustomize (executes arbitrary site customization code), and atexit._run_exitfuncs (triggers all registered exit handler callbacks). The fickling.load() API chains check_safety() into pickle.loads() as an explicit security gate; a LIKELY_SAFE verdict causes the payload to be deserialized and executed. This shares the same root cause as CVE-2026-22607 (cProfile), CVE-2025-67748 (pty), and CVE-2025-67747 (marshal/types). OvertlyBadEvals does not flag these modules because they are standard library imports. UnsafeImports does not flag them because they are not in the denylist. The UnusedVariables heuristic is defeated by the SETITEMS opcode pattern.	2026-07-04	8.8	CVE-2026-14534
trailofbits--fickling	In Trail of Bits fickling versions up to and including 0.1.11, the UnsafeImportsML analysis pass unconditionally calls AnalysisContext.shorten_code(node) on every import node it inspects, regardless of whether the import is flagged as unsafe. This call registers the shortened code representation in the shared AnalysisContext.reported_shortened_code set. When the MLAllowlist analysis pass subsequently runs, it calls the same shorten_code() method, receives already_reported=True for every import, and executes a continue statement that skips its allowlist check entirely. This renders MLAllowlist dead code for all imports - it never evaluates whether an import is in the ML allowlist or not. The MLAllowlist pass was designed to catch imports of modules outside the known-safe ML ecosystem (torch, numpy, transformers, etc.) that slip past the UnsafeImports denylist. With MLAllowlist inoperative, any standard library module not in the UNSAFE_IMPORTS denylist can be invoked via pickle deserialization while fickling's check_safety() returns LIKELY_SAFE. The fickling.load() API chains check_safety() into pickle.loads() as an explicit security gate, meaning a LIKELY_SAFE verdict causes the payload to be deserialized and executed. The root cause is shared mutable state between independently-correct analysis passes - UnsafeImportsML works as designed in isolation, MLAllowlist works as designed in isolation, but the shared reported_shortened_code set causes UnsafeImportsML to poison MLAllowlist's deduplication logic.	2026-07-04	8.8	CVE-2026-14535
tranmautritam--TheFox	Unauthenticated Cross Site Scripting (XSS) in TheFox <= 3.9.76 versions.	2026-07-02	7.1	CVE-2026-27430
TUBITAK BILGEM Software Technologies Research Institute--Pardus Domain Joiner	Invocation of process using visible sensitive information vulnerability in TUBITAK BILGEM Software Technologies Research Institute Pardus Domain Joiner allows Excavation. This issue affects Pardus Domain Joiner: from 0.5.2 before 0.5.4.	2026-07-05	7.9	CVE-2026-12250

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
TUBITAK BILGEM Software Technologies Research Institute--Pardus Update	Missing Authorization vulnerability in TUBITAK BILGEM Software Technologies Research Institute Pardus Update allows Privilege Escalation. This issue affects Pardus Update: from <=0.6.3 before 0.6.6.	2026-07-05	7.8	CVE-2026-6509
TUBITAK BILGEM Software Technologies Research Institute--Pardus-Parental-Control	Incorrect Permission Assignment for Critical Resource, Improper Access Control vulnerability in TUBITAK BILGEM Software Technologies Research Institute Pardus-Parental-Control allows DNS Spoofing. This issue affects Pardus-Parental-Control: from <=0.5.1 before 0.7.0.	2026-07-05	8.8	CVE-2026-9085
TUBITAK BILGEM Software Technologies Research Institute--pardus-software	Improper neutralization of argument delimiters in a command ('argument injection') vulnerability in TUBITAK BILGEM Software Technologies Research Institute pardus-software allows Argument Injection. This issue affects pardus-software: from <= 1.0.4 before 1.0.5.	2026-07-03	8.8	CVE-2026-14459
TUBITAK BILGEM Software Technologies Research Institute--pardus-software	Missing Authorization vulnerability in TUBITAK BILGEM Software Technologies Research Institute pardus-software allows Argument Injection. This issue affects pardus-software: from <= 1.0.4 before 1.0.5.	2026-07-03	8.8	CVE-2026-14460
Ubiquiti Inc--Dream Machines	A malicious actor with access to the network and under certain network configurations could exploit an Improper Access Control vulnerability found in certain devices running UniFi OS to make unauthorized changes to such UniFi OS devices.	2026-07-02	9	CVE-2026-55116
Ubiquiti Inc--Dream Machines	A malicious actor with access to the network and low privileges and under certain conditions could exploit an Improper Access Control vulnerability found in UniFi OS with UniFi Protect Application to escalate privileges on the host device.	2026-07-02	7.5	CVE-2026-55112
Ubiquiti Inc--UniFi Access Application	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi Access Application to execute a Command Injection on the host device.	2026-07-02	9.9	CVE-2026-50748
Ubiquiti Inc--UniFi Access Application	A malicious actor with access to the network and high privileges could exploit an Improper Access Control vulnerability found in UniFi Access Application to escalate privileges on the host device.	2026-07-02	9.1	CVE-2026-54400
Ubiquiti Inc--UniFi Access Application	A malicious actor with access to the network could exploit a Path Traversal vulnerability found in UniFi Access Application to access files on the host device.	2026-07-02	8.6	CVE-2026-55117
Ubiquiti Inc--UniFi Connect Application	A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi Connect Application to execute a Command Injection on the host device.	2026-07-02	10	CVE-2026-50746
Ubiquiti Inc--UniFi Network Application	A malicious actor with access to the network and high privileges could exploit a Path Traversal vulnerability found in self-hosted instances of UniFi Network Application to escalate write permission on the host device.	2026-07-02	8.7	CVE-2026-54406
Ubiquiti Inc--UniFi Network Application	A malicious actor with access to the network and low privileges could exploit an Improper Access Control vulnerability found in UniFi Network Application to escalate privileges within the UniFi Network Application.	2026-07-02	8.8	CVE-2026-55114
Ubiquiti Inc--UniFi Network Application	A malicious actor with access to the network,low privileges and under certain conditions could exploit an Improper Access Control vulnerability found in UniFi Network Application to escalate privileges within the UniFi Network Application.	2026-07-02	8.3	CVE-2026-55118
Ubiquiti Inc--UniFi Network Application	A malicious actor with access to the network could exploit an Improper Input Validation vulnerability found in UniFi Network Application to execute a Denial of Service (DoS) attack on the application.	2026-07-02	7.5	CVE-2026-54405

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Ubiquiti Inc-- UniFi Network Application	A malicious actor with access to the network and under certain conditions could exploit an Incorrect Authorization vulnerability found in UniFi Network Application to persist privileges within UniFi Network Application after such access had been removed.	2026-07-02	7.5	CVE-2026-56842
Ubiquiti Inc-- UniFi OS Server	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability found in UniFi OS to execute a Command Injection on the host device.	2026-07-02	9.9	CVE-2026-54402
Ubiquiti Inc-- UniFi OS Server	A malicious actor with access to the network could exploit a Path Traversal vulnerability found in certain devices running UniFi OS to bypass authentication of such UniFi OS devices or instances.	2026-07-02	8.6	CVE-2026-54403
Ubiquiti Inc-- UniFi OS Server	A malicious actor with access to the network and low privileges could exploit a series of authenticated SQL Injection vulnerabilities found in UniFi OS to escalate privileges within such UniFi OS devices or instances.	2026-07-02	8.8	CVE-2026-54404
Ubiquiti Inc-- UniFi OS Server	A malicious actor with access to the network and low privileges could exploit a Server-Side Request Forgery (SSRF) to escalate privileges within such UniFi OS devices or instances.	2026-07-02	7.7	CVE-2026-54401
Ubiquiti Inc-- UniFi OS Server	A malicious actor who lures an authenticated user to a malicious page could exploit a Cross-Origin Resource Sharing (CORS) misconfiguration found in UniFi OS to trigger actions in UniFi OS using that user's session.	2026-07-02	7.5	CVE-2026-55110
Ubiquiti Inc-- UniFi Protect Application	A malicious actor with access to the network and low privileges could exploit a Server-Side Request Forgery (SSRF) in UniFi Protect Application to escalate privileges on the host device.	2026-07-02	9.9	CVE-2026-55115
Ubiquiti Inc-- UniFi Protect Application	A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi Protect Application to bypass authentication in certain UniFi Protect Application API endpoints.	2026-07-02	8.6	CVE-2026-54407
Ubiquiti Inc-- UniFi Protect Application	A malicious actor with access to the network could exploit an Improper Access Control vulnerability found in UniFi Protect Application to bypass authentication for data streaming.	2026-07-02	8.6	CVE-2026-54408
Ubiquiti Inc-- UniFi Protect Application	A malicious actor with access to the network and low privileges could exploit an authenticated SQL Injection vulnerability found in UniFi Protect Application to escalate privileges on the host device.	2026-07-02	8.8	CVE-2026-56841
Ubiquiti Inc-- UniFi Protect Application	A malicious actor with access to the network and under certain conditions could exploit an Improper Initialization vulnerability found in UniFi Protect Application to bypass authentication in UniFi Protect Cameras.	2026-07-02	7.5	CVE-2026-54409
Ubiquiti Inc-- UniFi Protect Floodlight	A malicious actor with access to the network could exploit a Path Traversal vulnerability found in UniFi Protect Floodlight devices to access files on the UniFi Protect Floodlight.	2026-07-02	7.5	CVE-2026-55111
Ubiquiti Inc-- UniFi Talk Application	A malicious actor with access to the network and low privileges could exploit a series of authenticated SQL Injection vulnerabilities found in UniFi Talk Application to escalate privileges on the host device.	2026-07-02	9.9	CVE-2026-50747
Ubiquiti Inc-- UniFi Talk Application	A malicious actor with access to the network and low privileges could exploit an Improper Access Control vulnerability found in UniFi Talk Application to escalate privileges within the UniFi Talk Application.	2026-07-02	8.1	CVE-2026-55119
Ubiquiti Inc-- UniFi Talk Application	A malicious actor with access to the network could exploit a Server-Side Request Forgery (SSRF) vulnerability found in UniFi Talk Application to execute a Denial of Service (DoS) attack and bypass authentication in certain UniFi Talk API endpoints.	2026-07-02	7.5	CVE-2026-55113
Unisoc (Shanghai) Technologies Co., Ltd.-- SC7731E/SC9832E/SC9863A/T310/T610/T618/T7200/T7225/T7250/T7255/T7280/T7300/T8100/T9100/T8200/T8300	In IMS, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed.	2026-07-03	7.5	CVE-2026-4967

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Unity--Parsec	An Incorrect Use of Privileged APIs vulnerability in Unity Parsec on Windows hosts leads to a potential Elevation of Privilege. This issue affects Parsec through v2026-05-04.0. The patched version is Parsec for Windows version 150-104a. A user can generate a situation where there is an instance of parsecd.exe running as NT AUTHORITY\SYSTEM with a user-controlled value of the AppData environment variable.	2026-07-04	8.4	CVE-2026-54424
UTT--HiPER 1250GW	A vulnerability has been found in UTT HiPER 1250GW up to 3.2.7-210907-180535. This affects an unknown function of the file /goform/ConfigWirelessBase_5g of the component Web Endpoint. The manipulation of the argument ssid leads to stack-based buffer overflow. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	2026-07-05	8.8	CVE-2026-14721
uvnc--UltraVNC	UltraVNC repeater through 1.8.2.2 initializes the HTTP administration server with a hardcoded default password. In repeater/webgui/settings.c:197, when settings2.txt is absent on first run the repeater writes the literal string "adminadmi2" as the admin password via strcpy_s(saved_password, 64, "adminadmi2"). The HTTP Basic-auth handler wi_decode_auth() checks this password without rate-limiting or lockout. Any remote attacker who can reach the repeater HTTP port (default TCP 80) can authenticate as administrator using the well-known default credential on a fresh or unmodified installation, gaining full control of the repeater configuration including allow/deny rules and session visibility.	2026-07-01	9.1	CVE-2026-7839
uvnc--UltraVNC	UltraVNC repeater through 1.8.2.2 contains a global buffer overflow in its embedded HTTP administration server. The functions wi_senderr() and wi_replyhdr() in repeater/webgui/webutils.c write the caller-supplied HTTP request URI into a fixed 1000-byte global buffer (hdrbuf) via unchecked sprintf calls. The HTTP receive buffer accepts URIs up to approximately 150 KB (WI_RXBUFSIZE = 153600), so an unauthenticated attacker who can reach the repeater HTTP port (default TCP 80) can overflow hdrbuf by at least 500 bytes with a single HTTP request containing a URI of 1500 bytes or longer, corrupting adjacent .bss-segment globals. The overflow occurs before any authentication check, making it reachable without credentials. A remote, unauthenticated attacker can achieve arbitrary code execution on the host running the repeater.	2026-07-01	9.8	CVE-2026-7840
uvnc--UltraVNC	UltraVNC viewer through 1.8.2.2 contains an integer overflow leading to a heap buffer overflow in the RFB protocol failure-response parsing path. In vncviewer/ClientConnection.cpp, the 4-byte network-supplied reasonLen field (type CARD32) is passed as reasonLen+1 to CheckBufferSize(). Because both operands are unsigned 32-bit, a reasonLen of 0xFFFFFFFF overflows to 0, causing CheckBufferSize to allocate only 256 bytes. The subsequent ReadString(m_netbuf, reasonLen) call then performs ReadExact for the original 4 GiB length into that 256-byte heap buffer. This overflow is reachable via rfbConnFailed (auth-scheme negotiation) and rfbVncAuthFailed (post-handshake) message types without successful authentication. A malicious VNC server, or any man-in-the-middle on the RFB stream, can trigger this condition when the victim viewer connects, potentially resulting in remote code execution as the user running the viewer. The crash was confirmed with AddressSanitizer on a portable reproduction harness (heap-buffer-overflow WRITE at offset 256).	2026-07-01	8.8	CVE-2026-7838
uvnc--UltraVNC	UltraVNC repeater through 1.8.2.2 contains a post-authentication out-of-bounds write in the allow/deny rule parser. In repeater/webgui/settings.c:225-272, after strncpy_s copies a rule token into temp1[rule1] (25-byte destination) or temp2/temp3 (16-byte destination), the code unconditionally writes a NUL terminator at temp1[rule1][len] = 0 without clamping len to the destination size. When an authenticated administrator saves a rule with a token length equal to or greater than the destination size, the NUL byte is written one or more bytes past the end of the stack-allocated array, corrupting adjacent stack	2026-07-01	7.2	CVE-2026-7829

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	data. An attacker who has obtained admin credentials (including via CVE-2026-7839 default password) can trigger this to gain code execution on the repeater host.			
uvnc--UltraVNC	UltraVNC through 1.8.2.2 uses inadequate cryptography in the MS-Logon II authentication scheme (rfbUltraVNC_MsLogonIIAuth). In rfb/dh.cpp the Diffie-Hellman key exchange is performed with parameters that fit in an unsigned 64-bit integer (DH_MAX_BITS controls the prime size). A 64-bit DH key can be broken by Pollard's rho algorithm in under one second on current hardware. Additionally, the private exponent is generated by the rng() function, which multiplies three libc rand() values seeded from time(NULL). With approximately 31 bits of internal state and a time-based seed, the private exponent is recoverable in under a minute by a passive observer. A network attacker who can observe the MS-Logon II handshake (via sniffing, recording, or man-in-the-middle) can derive the shared DH key and decrypt the encapsulated username and password, resulting in full credential disclosure. This affects legacy MS-Logon II connections; MS-Logon III (X25519 + AES-256-GCM) is unaffected.	2026-07-01	7.4	CVE-2026-7830
uvnc--UltraVNC	UltraVNC viewer through 1.8.2.2 contains an off-by-one stack buffer overflow in the RFB ServerInit message handler. In vncviewer/ClientConnection.cpp, when the server-supplied nameLength equals exactly 2024 the code declares a 2024-byte stack buffer _dn[2024] and calls ReadString(_dn, 2024). ReadString writes the NUL terminator at buf[length], i.e., _dn[2024], one byte past the end of the stack buffer. A malicious VNC server can trigger this condition by advertising a desktop name of length 2024 in its ServerInit message. On release builds without stack canaries the single-byte NUL overwrite adjacent stack data. On builds with /GS stack protection the canary is corrupted and the process terminates, resulting in denial of service. User interaction (connecting the viewer to the malicious server) is required.	2026-07-01	7.5	CVE-2026-7831
videowhisper--Paid Videochat Turnkey Site	Performer Arbitrary File Deletion in Paid Videochat Turnkey Site <= 7.4.8 versions.	2026-06-29	9.9	CVE-2026-57331
wagtail--wagtail	Wagtail is an open source content management system built on Django. In versions prior to 7.0.8, 7.3.3 and 7.4.2, reflected cross-site scripting (XSS) vulnerability exists on the dynamic image URL generator view within the Wagtail admin interface. A user with a limited-permission editor account for the Wagtail admin could craft a URL that, when viewed by a user with higher privileges, could perform actions with that user's credentials. The vulnerability is present for all sites, even if they do not enable the dynamic image serve view. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. This issue has been fixed in versions 7.0.8, 7.3.3, and 7.4.2.	2026-07-01	7.3	CVE-2026-54263
Wavlink--WL-NU516U1-A	A vulnerability was identified in Wavlink WL-NU516U1-A M16U1_V240425. The impacted element is the function sub_407504 of the file /cgi-bin/wireless.cgi of the component POST Parameter Handler. Such manipulation of the argument Guest_ssid leads to stack-based buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be used. It is suggested to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	2026-06-29	8.8	CVE-2026-13539
weaviate--weaviate	Weaviate before 1.38.0 does not verify that a principal performing an RBAC role assignment holds the permissions granted by the assigned role. The assignRoleToUser and assignRoleToGroup handlers (POST /authz/users/{id}/assign and /authz/groups/{id}/assign) authorize only that the caller may assign roles to the target user or group, not the permissions contained in the assigned roles, unlike role creation which enforces that a user can only create roles with permissions less than or equal to its own. A user holding only the delegated	2026-07-02	8.8	CVE-2026-59093

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	assign_and_revoke_users or assign_and_revoke_groups permission can assign the built-in admin role, or any high-privilege custom role, to itself or others, escalating to full administrative control of the database.			
webandprint--AR for WooCommerce	The AR for WooCommerce plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 8.40 via the 'file' parameter parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. The three intended access controls all fail: valid nonces are freely minted by unauthenticated callers via the nopriv ar_get_fresh_nonce and ar_process_user_image AJAX handlers; the AES-256-CBC encryption key is derived from get_option('ar_licence_key'), which returns false on default free installations and yields a predictable key attackers can use to encrypt their own path payloads; and the Referer check is trivially bypassed because the Referer header is attacker-controlled.	2026-07-03	7.5	CVE-2026-14352
webandprint--AR for WordPress	The AR for WordPress plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 8.40 via the 'file' parameter parameter. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information. Exploitation requires an attacker to first obtain a valid nonce and secure nonce via the publicly accessible ar_get_fresh_nonce and ar_process_user_image nopriv AJAX handlers, and to reproduce the encryption key locally - both steps are fully achievable by an unauthenticated attacker on any default free or unlicensed installation where ar_licence_key is unset.	2026-07-03	7.5	CVE-2026-14327
webaways--NEX-Forms Ultimate Forms Plugin for WordPress	The NEX-Forms - Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via '_name[]' Array Parameter in all versions up to, and including, 9.2.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The wp_kses() output filtering pass provides no mitigation because NEXForms_allowed_tags() explicitly permits <script>, <iframe src/srcdoc>, and JS event handlers such as onClick, onBlur, and onChange in its allow-list.	2026-07-01	7.2	CVE-2026-12142
webaways--NEX-Forms Ultimate Forms Plugin for WordPress	The NEX-Forms - Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'real_val__' parameter in all versions up to, and including, 9.2.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The submission endpoint is registered via wp_ajax_nopriv_submit_nex_form with no nonce verification, making it fully accessible to unauthenticated attackers without any CSRF token.	2026-07-03	7.2	CVE-2026-13040
Webraketen--Internal Links Manager	Unauthenticated Cross Site Scripting (XSS) in Internal Links Manager <= 3.0.3 versions.	2026-07-02	7.1	CVE-2026-57345
wedevs--Dokan Pro	The Dokan Pro plugin for WordPress is vulnerable to privilege escalation via update_capabilities REST Endpoint in all versions up to, and including, 5.0.4. This is due to the `update_capabilities()` REST handler accepting arbitrary capability strings from the request body and passing them directly to WP_User::add_cap() with no allowlist validation, only verifying that the caller holds the dokandar capability. This makes it possible for authenticated attackers with a self-provisioned Vendor-level access and above, on sites with the Vendor Staff module enabled, to grant arbitrary WordPress capabilities, including administrator, to any vendor_staff account, leading to a full site takeover.	2026-07-01	8.8	CVE-2026-12224
woodpecker-ci--woodpecker	Woodpecker before 3.15.0 matches the ApprovalAllowedUsers bypass list against pipeline.Author. For the GitLab forge driver, pipeline.Author is populated from the git commit author name (commit.author.name)	2026-06-30	8.1	CVE-2026-58370

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	carried in the webhook payload, which is attacker-controlled and not verified by GitLab. A user who can open a merge request from a fork can set the commit author name to match an entry in ApprovalAllowedUsers, causing needsApproval to return false so the pipeline runs without the required approval. This defeats the fork-approval security boundary and allows execution of attacker-controlled pipeline steps on a Woodpecker agent and exfiltration of CI secrets exposed to the run. Other built-in forge drivers (Gitea, Forgejo, GitHub, Bitbucket) derive pipeline.Author from the forge-validated sender/actor identity and are not affected.			
WP Swings--Wallet System for WooCommerce	Subscriber Broken Access Control in Wallet System for WooCommerce <= 2.7.6 versions.	2026-06-29	7.1	CVE-2026-57332
WPXPO--WowAddons	Unauthenticated Cross Site Scripting (XSS) in WowAddons <= 1.6.14 versions.	2026-07-02	7.1	CVE-2026-57686
xndan--jodit	Jodit Editor is a WYSIWYG editor with written in pure TypeScript file and image editing capabilities. In versions prior to 4.12.28, the built-in clean-html sanitizer can be bypassed by a MathML/<style> carrier that hides a dangerous element from the sanitizer's element walk, so a no-interaction event handler survives into the editor value, potentially causing Mutation XSS. When an application supplies attacker-influenced HTML to the editor's value-set or insertion paths, the sanitized output still contains a live (or another non-onerror handler such as onfocus). A consumer that renders that output (element.innerHTML = editor.value) executes the handler with no user interaction. This issue has been fixed in version 4.12.28.	2026-07-01	7.2	CVE-2026-58263
XplodedThemes--WPIDE File Manager & Code Editor	Unauthenticated Cross Site Request Forgery (CSRF) in WPIDE - File Manager & Code Editor <= 3.5.6 versions.	2026-07-02	8.8	CVE-2026-57766
Yonyou Network Technology Co., Ltd.--KSOA	Yonyou KSOA 9.0 contains an unauthenticated arbitrary file upload vulnerability in the com.sksoft.bill.ImageUpload servlet that allows unauthenticated attackers to upload arbitrary files by submitting a POST request with attacker-controlled filepath and filename parameters without any authentication, file type, extension, or content validation. Attackers can upload a JSP webshell by specifying a malicious filename and root filepath, with the uploaded file stored under the pictures directory and directly executed by the web server, resulting in unauthenticated remote code execution. Exploitation evidence was first observed by the Shadowserver Foundation on 2023-11-07 (UTC).	2026-07-02	9.8	CVE-2022-50973
Yunai--ruoyi-vue-pro	ruoyi-vue-pro through 2026.05, fixed in commit 5d1fd70 contains a broken access control vulnerability in ErpSaleOrderController that allows attackers with erp:sale-out permissions to gain unauthorized access to sale order operations by exploiting an incorrect permission namespace enforcement. Attackers holding shipment-level permissions can perform unauthorized create, update, delete, and read operations on financially sensitive sale orders due to the controller enforcing erp:sale-out instead of the intended erp:sale-order namespace.	2026-06-29	8.1	CVE-2026-57950
YunaiV--ruoyi-vue-pro	A vulnerability was found in YunaiV/zhijiantianya ruoyi-vue-pro up to 2026.04-jdk8-SNAPSHOT. The impacted element is the function generateUploadPath of the file yudao-module-infra/src/main/java/cn/iocoder/yudao/module/infra/service/file/FileServiceImpl.java of the component AppFileController File Upload Endpoint. Performing a manipulation results in path traversal. Remote exploitation of the attack is possible. The exploit has been made public and could be used. The patch is named 4ae3f6b2c9883978837638c14e3d18419819eeb0. It is recommended to apply a patch to fix this issue. This product is published by multiple vendors.	2026-06-29	7.3	CVE-2026-13528

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
zedeus--nitter	Nitter's /video media proxy endpoint fails to validate target URLs against Twitter/X domains and uses a hardcoded default HMAC key, allowing unauthenticated attackers to compute valid HMACs for arbitrary URLs. Attackers can retrieve HTTP responses from any host reachable by the server, including cloud metadata services and internal network resources.	2026-06-29	8.6	CVE-2026-56285
zephyrproject--zephyr	The IPv6 Neighbor Discovery handlers in subsys/net/ip/ipv6_nbr.c (handle_ra_input, handle_ns_input, handle_na_input) used an incorrect boolean expression that combined the RFC 4861 validity checks with the ICMPv6 code check using the wrong operator precedence: the form was '((length/hop/source/target checks) && (icmp_hdr-code != 0))'. Because every legitimate ND message carries ICMPv6 code 0, an attacker setting code == 0 (the normal value) caused the entire predicate to evaluate false, so the packet was never dropped and all of the other checks were silently skipped. The bypassed checks include the mandatory Hop Limit == 255 verification (which proves an ND packet originated on-link and was not forwarded) and, for Router Advertisements, the requirement that the source be a link-local address, as well as multicast-target sanity checks. As a result, an adjacent on-link attacker - and, because the Hop-Limit-255 guard is bypassed, potentially a remote/off-link attacker whose packets would otherwise be rejected - can have forged Router Advertisement, Neighbor Solicitation, and Neighbor Advertisement messages accepted. A forged RA lets the attacker reconfigure the victim's default router, on-link prefixes (SLAAC), MTU, reachable/retransmit timers, and (with CONFIG_NET_IPV6_RA_RDNSS) DNS servers, while forged NS/NA enable neighbor-cache poisoning, enabling man-in-the-middle, traffic redirection, and denial of service. The flaw is an input-validation/authentication weakness rather than a memory-safety issue: the underlying packet-parsing primitives (net_pkt_get_data, net_pkt_read, net_pkt_skip) are independently bounds-safe and the validated 'length' is the true buffer length, so skipping the length check causes no out-of-bounds access. The defect has existed since the logic was introduced in 2018 and shipped in all releases through v4.4.0; it is fixed by splitting the condition so any failing check drops the packet.	2026-06-29	8.1	CVE-2026-7656
zephyrproject--zephyr	Zephyr's HTTP server (subsys/net/lib/http) provides a static-filesystem resource type (HTTP_RESOURCE_TYPE_STATIC_FS, available when CONFIG_FILE_SYSTEM is enabled) that serves files from a configured root directory. Before this fix, both the HTTP/1 and HTTP/2 front-ends placed the raw, attacker-controlled request path into client-url_buffer (assembled in on_url() for HTTP/1 and copied verbatim from the :path pseudo-header for HTTP/2) without resolving ../ segments. The static-FS handler then built the on-disk filename by directly concatenating the configured root with that raw URL (snprintf(fname, ..., "%s%s", static_fs_detail-fs_path, client-url_buffer) at http_server_http1.c:603 and http_server_http2.c:490) and opened it with fs_open(fname, FS_O_READ). Because the handler is reached via wildcard/leading-dir (fnmatch FNM_LEADING_DIR) or fallback resource matching, a request such as GET /<prefix/../../<file is dispatched to the handler and, after the underlying filesystem (e.g. LittleFS/FAT) resolves the .. segments, escapes the configured web root, letting an unauthenticated remote client read arbitrary readable files on the mounted volume (information disclosure). The HTTP server requires no TLS or authentication to reach this path. The fix adds http_server_remove_dot_segments(), which canonicalizes the path portion of the URL before resource lookup in both protocol handlers, neutralizing the traversal. Affects releases v4.0.0 through v4.4.0 for deployments that register a static-filesystem resource.	2026-06-29	7.5	CVE-2026-8023
Zoothermes--Zegen	Subscriber Arbitrary File Upload in Zegen <= 1.1.9 versions.	2026-07-02	9.9	CVE-2026-27419

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
10web--Photo Gallery by 10Web Mobile-Friendly Image Gallery	The Photo Gallery by 10Web - Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to time-based SQL Injection via 'compact_album_order_by' Shortcode Parameter in all versions up to, and including, 1.8.41 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The malicious payload is stored via the 'shortcode_bwg' AJAX handler - accessible to Contributor-level users and exploitable without a valid nonce by omitting the 'page' parameter - and is subsequently triggered by the unauthenticated 'bwg_frontend_data' AJAX handler, meaning successful exploitation requires only that an attacker has Contributor-level access to save the shortcode.	2026-06-06	6.5	CVE-2026-9829
a4m4--Student-Management-System	A flaw has been found in a4m4 Student-Management-System up to f0c5f6842c5e8c431ff02b5260a565ca844df3a0. The affected element is an unknown function of the file admin/ of the component Admin Endpoint. This manipulation of the argument uid causes execution after redirect. It is possible to initiate the attack remotely. The exploit has been published and may be used. This product is using a rolling release to provide continuous delivery. Therefore, no version details for affected nor updated releases are available. Multiple endpoints are affected. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	6.3	CVE-2026-10271
a4m4--Student-Management-System	A vulnerability has been found in a4m4 Student-Management-System up to f0c5f6842c5e8c431ff02b5260a565ca844df3a0. The impacted element is an unknown function of the file admin/deleteform.php. Such manipulation of the argument sid leads to improper authorization. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This product takes the approach of rolling releases to provide continuous delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	6.5	CVE-2026-10272
absikandar--Frontend User Notes	The Frontend User Notes plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1.1. This is due to missing or incorrect nonce validation on the funp_ajax_modify_notes function. This makes it possible for unauthenticated attackers to trick a logged-in user into visiting a malicious page, causing unauthorized overwriting of that victim's own note content via a forged cross-site request to wp_update_post() via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Due to ownership enforcement comparing the note's stored _funp_single_user_id meta against the current session's user ID, the attack is limited to modifying only notes belonging to the tricked victim, and cannot be used to alter notes owned by arbitrary third-party users.	2026-06-05	4.3	CVE-2026-7047
ahujasid--blender-mcp	A vulnerability was found in ahujasid blender-mcp up to 7636d13bded82eca58eb93c3f4cd8708dfdfbe8b. The affected element is the function requests.get of the file src/blender_mcp/server.py of the component ZIP File Handler. The manipulation of the argument zip_file_url	2026-06-02	6.3	CVE-2026-10662

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	results in server-side request forgery. The attack can be executed remotely. The exploit has been made public and could be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The patch is identified as 5b37be25242e73dc4cf1328974d30458b9e5d67e. It is advisable to implement a patch to correct this issue.			
ahujasid--blender-mcp	A vulnerability was determined in ahujasid blender-mcp up to 7636d13bded82eca58eb93c3f4cd8708dfdfbe8b. The impacted element is the function execute_blender_code of the file /src/blender_mcp/server.py. This manipulation of the argument code causes code injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-02	5.5	CVE-2026-10688
ahujasid--blender-mcp	A vulnerability has been found in ahujasid blender-mcp up to 7636d13bded82eca58eb93c3f4cd8708dfdfbe8b. Impacted is the function Open of the file src/blender_mcp/server.py. The manipulation of the argument input_image_url leads to injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The identifier of the patch is 5b37be25242e73dc4cf1328974d30458b9e5d67e. To fix this issue, it is recommended to deploy a patch.	2026-06-02	4.3	CVE-2026-10661
aio-libs--aiohttp	AIOHTTP is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.14.0, using ``CookieJar.load()`` with untrusted input may allow arbitrary code execution. Most applications using this function will be doing so with the user's own data, so this is unlikely to affect many applications. Version 3.14.0 patches the issue. If an application does allow attacker controlled files to be loaded, a workaround on older releases would be to sanitize the files before loading.	2026-06-02	6.4	CVE-2026-34993
alejo30--Alba Board	The Alba Board plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.1.3. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to access arbitrary private alba_card post data, including title, description, assignee, due date, tags, and comments, that is intended to be restricted to Administrators and Editors. The handler is registered via the wp_ajax_nopriv_hook and its nonce is exposed to all site visitors through wp_localize_script on pages containing the [alba_board] shortcode, making this exploitable by unauthenticated users who can access any such page.	2026-06-05	4.3	CVE-2026-7523
alfio-event--alf.io	alf.io is an open source ticket reservation system for conferences, trade shows, workshops, and meetups. Prior to version 2.0-M5-2606, the alf.io extension sandbox injects a fully-functional HTTP client ('simpleHttpClient') into every extension script's scope. The 'postFileAndSaveResponse()' method accepts an arbitrary filesystem path as its 'file' parameter and reads the file contents using 'new	2026-06-02	4.9	CVE-2026-41412

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	FileInputStream(file)` with no path validation, directory restriction, or allowlist. A malicious extension script can read any file accessible to the JVM process user and exfiltrate it to an attacker-controlled server via HTTP POST. Version 2.0-M5-2606 patches the issue.			
Anton Shevchuk-Constructor	Missing Authorization vulnerability in Anton Shevchuk Constructor allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Constructor: from n/a through 1.6.5.	2026-06-02	5.3	CVE-2025-53302
Appsmith--Appsmith	Appsmith's SQL query editor's autocomplete functionality fails to sanitize database object names before rendering them in innerHTML, allowing an authenticated Developer to inject persistent XSS by a malicious table or column names triggering arbitrary code execution in the sessions of other workspace members when they interact with the same datasource.	2026-06-02	6.3	CVE-2026-7299
Arista Networks--Arista Edge Threat Management - Arista Next Generation Firewall (NGFW)	An encrypted password command injection vulnerability exists in the Captive Portal application framework of Arista Edge Threat Management - Arista Next Generation Firewall (NGFW). This issue uniquely affects version 17.4.0; earlier software releases are not exposed.	2026-06-05	6	CVE-2026-25620
Arista Networks--Arista Edge Threat Management - Arista Next Generation Firewall (NGFW)	A Reports application infrastructure vulnerability exists in Arista Edge Threat Management - Arista Next Generation Firewall (NGFW) due to insecure input validation. This issue uniquely affects version 17.4.0; earlier software releases are not exposed.	2026-06-05	6	CVE-2026-25621
Arista Networks--Arista Edge Threat Management - Arista Next Generation Firewall (NGFW)	A Captive Portal Custom Handler command injection vulnerability exists in Arista Edge Threat Management - Arista Next Generation Firewall (NGFW). On affected platforms, an administrative account logged into the user interface can exploit this input handling behavior to execute arbitrary platform shell commands.	2026-06-05	6	CVE-2026-25622
Arista Networks--Arista Edge Threat Management - Arista Next Generation Firewall (NGFW)	An input validation command execution vulnerability exists in the browser management pipeline of Arista Edge Threat Management - Arista Next Generation Firewall (NGFW). Authenticated administrators can leverage this exposure to obtain underlying terminal script code processing execution permissions.	2026-06-05	6	CVE-2026-25623
Arista Networks--Arista Edge Threat Management - Arista Next Generation Firewall (NGFW)	An administrative cross-site scripting (XSS) vulnerability exists in the web user interface dashboard layout of Arista Edge Threat Management - Arista Next Generation Firewall (NGFW). Unvalidated user-supplied variables are echoed back to administrative profiles, facilitating vector payload processing behavior controls.	2026-06-05	5.7	CVE-2026-25624

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Arista Networks-EOS	On affected platforms running Arista EOS with 802.1x authentication configured on the access/trunk ports, and routing enabled on the access VLAN of the ports, a malicious supplicant may be able to bypass the requirement to perform 802.1x authentication.	2026-06-04	5.9	CVE-2023-5502
Arista Networks-EOS	On affected platforms running Arista EOS with MACsec and egress ACLs configured on the same interfaces, the ACL policies may not be enforced for packets egressing on those ports. This can cause outgoing packets to incorrectly be allowed or denied.	2026-06-04	5.3	CVE-2024-27891
Arista Networks-EOS	On affected platforms with hardware IPsec support running Arista EOS with certain IPsec features enabled, EOS may exhibit unexpected behavior in specific cases. Physical interface flaps and certain agent restarts can cause IPsec tunnel re-establishment with existing Security Associations, resulting in sequence number mismatches between tunnel endpoints potentially causing unstable communication.	2026-06-05	5.9	CVE-2026-2379
Arista Networks-EOS	On affected platforms running Arista EOS where a tunnel decapsulation configuration-such as VXLAN (Virtual Extensible LAN), decap-groups, or a GRE (Generic Routing Encapsulation) tunnel interface-is present, the switch will incorrectly decapsulate and forward other unexpected tunneled packet with a destination IP matching its configured decapsulation IP. This occurs because the switch does not verify the tunnel protocol type, potentially leading to the unexpected processing of non-configured tunnel traffic. This issue has been reported as being exploited in the wild.	2026-06-05	5.8	CVE-2026-7473
Arista Networks-EOS / CloudVision eXchange (CVX)	In a CVX cluster, an EOS switch connected to a CVX server is not resilient to certain malformed messages received from the connected CVX server. Similarly, the CVX server is not resilient to certain malformed messages received from the connected EOS switch. This leads to either a Sysdb agent crash on the EOS device causing a soft reset of the switch or agent crashes on the CVX server causing instability of the CVX cluster. An attacker could use this behavior to create a denial of service (DoS) scenario. Note that this would require the attacker to already have a high privilege access to the connected device to be able to send custom TCP packets. EOS switches that are not connected to a CVX server are not impacted.	2026-06-05	6.5	CVE-2025-5089
Arista Networks-EOS / CloudVision eXchange (CVX)	CVX is not resilient to unexpected messages from a connected switch. This leads to agent crashes on CVX causing instability in the CVX cluster. An attacker could use this behavior to create a denial of service (DoS) scenario. Note that this would require the attacker to have a high privilege access to the connected switch to be able to send custom TCP packets to the CVX.	2026-06-05	6.5	CVE-2025-5090
ariyes--WP Nano AD	The WP Nano AD plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'blogrole_link' parameter in all versions up to, and including, 1.31 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2026-06-02	5.5	CVE-2025-5085
armember--ARMember Premium	The ARMember Premium plugin for WordPress is vulnerable to SQL Injection via the 'sSortDir_0' parameter of the 'get_private_content_data' AJAX action in all versions up to, and including, 7.3.1. This is due to	2026-06-02	6.5	CVE-2026-5074

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Membership Plugin, Content Restriction, Member Levels, User Profile & User signup	insufficient sanitization of the user-supplied parameter which is concatenated directly into the ORDER BY clause of an SQL query without a whitelist check. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Note: The vulnerability can only be exploited if the "User Private Content" addon is enabled, which is disabled by default..			
arunbasillal--Auto Image Attributes From Filename With Bulk Updater (Add Alt Text, Image Title For Image SEO)	The Auto Image Attributes From Filename With Bulk Updater (Add Alt Text, Image Title For Image SEO) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the attachment metadata in all versions up to, and including, 4.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-02	6.4	CVE-2026-3722
Assimp--Assimp	A vulnerability was determined in Assimp up to 6.0.4. This affects the function HL1MDLLoader::read_meshe of the file HL1MDLLoader.cpp of the component Half-Life 1 MDL Loader. This manipulation causes heap-based buffer overflow. The attack is restricted to local execution. The exploit has been publicly disclosed and may be utilized. The project tagged the reported issue as bug.	2026-06-01	5.3	CVE-2026-10229
Assimp--Assimp	A vulnerability was identified in Assimp up to 6.0.4. This impacts the function Assimp::MDL::HalfLife::HL1MDLLoader::read_animations of the file HL1MDLLoader.cpp of the component Half-Life 1 MDL Loader. Such manipulation leads to heap-based buffer overflow. The attack must be carried out locally. The exploit is publicly available and might be used. The project tagged the reported issue as bug.	2026-06-01	5.3	CVE-2026-10230
Assimp--Assimp	A security flaw has been discovered in Assimp up to 6.0.4. Affected is the function HL1MDLLoader::extract_anim_value of the file HL1MDLLoader.cpp of the component Half-Life 1 MDL Loader. Performing a manipulation of the argument num.total results in heap-based buffer overflow. The attack must be initiated from a local position. The exploit has been released to the public and may be used for attacks. The project tagged the reported issue as bug.	2026-06-01	5.3	CVE-2026-10231
Assimp--Assimp	A weakness has been identified in Assimp up to 6.0.4. Affected by this vulnerability is the function aiNode::~aiNode of the file scene.cpp of the component ASE File Parser. Executing a manipulation can lead to use after free. The attack needs to be launched locally. The exploit has been made available to the public and could be used for attacks. The project tagged the reported issue as bug.	2026-06-01	5.3	CVE-2026-10232
AstrBotDevs--AstrBot	A vulnerability was found in AstrBotDevs AstrBot 4.23.6. Affected by this vulnerability is the function _sanitize_prompt_description of the file astrbot/core/skills/skill_manager.py. The manipulation results in injection. The attack may be performed from remote. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-01	6.3	CVE-2026-10210
AstrBotDevs--AstrBot	A vulnerability was determined in AstrBotDevs AstrBot 4.23.6. Affected by this issue is the function _normalize_rw_path of the file astrbot/core/tools/computer_tools/fs.py. This manipulation causes	2026-06-01	6.3	CVE-2026-10211

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	incorrect authorization. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.			
AstrBotDevs--AstrBot	A vulnerability was identified in AstrBotDevs AstrBot 4.24.2. This affects the function astr_main_agent of the file astrbot/core/astr_main_agent.py. Such manipulation of the argument session_id leads to authorization bypass. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-01	6.3	CVE-2026-10212
AstrBotDevs--AstrBot	A security flaw has been discovered in AstrBotDevs AstrBot 4.23.6. This vulnerability affects unknown code of the file /api/skills/delete of the component API Endpoint. Performing a manipulation of the argument Name results in path traversal. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-01	5.4	CVE-2026-10213
awordpresslife--Event Monster Event Manager, Ticket Booking & Registration	The Event Monster - Event Management, Events Calendar, Tickets plugin for WordPress is vulnerable to Insufficient Verification of Data Authenticity in versions up to, and including, 2.1.0. This is due to the capture_payment() AJAX handler (registered via wp_ajax_nopriv_em_capture_payment) trusting client-supplied payment data - including transaction ID, amount, and payment status - without performing any server-side verification against the PayPal API or any other payment gateway, and without nonce or capability checks. This makes it possible for unauthenticated attackers to forge payment records, mark bookings as Completed, and obtain confirmation emails containing valid QR code tickets without making any actual payment.	2026-06-05	5.3	CVE-2026-8608
AWS--Graph Explorer	Proxy server in Graph Explorer before 3.0.1 falls back to HTTP when certificate files are missing, which might allow remote threat actors to obtain sensitive information via interception of requests intended to be sent over HTTPS. To remediate this issue, users should upgrade to Graph Explorer v3.0.1 or later.	2026-06-02	5.9	CVE-2026-10584
birdseedapp--BirdSeed	The BirdSeed plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.2.0. This is due to missing nonce validation in the birdseed_plugin_settings_page() function. The function processes the 'birdseed_token' GET parameter and saves it to the database via update_option() without verifying a nonce. This makes it possible for unauthenticated attackers to change the plugin's BirdSeed token setting via a forged request, granted they can trick a site administrator into performing an action such as clicking a link.	2026-06-02	4.3	CVE-2026-4071
Bottelet--DaybydayCRM	A vulnerability was detected in Bottelet DaybydayCRM up to 2.2.1. Affected is an unknown function of the component Setting Handler. Performing a manipulation results in missing authentication. Remote exploitation of the attack is possible. It is recommended to apply a patch to fix this issue.	2026-06-01	6.3	CVE-2026-10283
Bottelet--DaybydayCRM	A security vulnerability has been detected in Bottelet DaybydayCRM up to 2.2.1. This impacts the function view of the file app/Http/Controllers/DocumentsController.php. Such manipulation leads	2026-06-01	4.3	CVE-2026-10282

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to improper authorization. The attack may be launched remotely. It is best practice to apply a patch to resolve this issue.			
browserstack-- browserstack-runner	BrowserStack Runner through 0.9.5 contains a path traversal vulnerability in the <code>_default</code> HTTP handler in <code>lib/server.js</code> that allows unauthenticated network-adjacent attackers to read arbitrary files. Attackers can exploit the unauthenticated HTTP server bound on all interfaces to traverse outside the project root and access sensitive files.	2026-06-02	6.5	CVE-2026-49144
chrisvrichardson-- MapPress Maps for WordPress	The MapPress Maps for WordPress plugin for WordPress is vulnerable to Authorization Bypass Through User-Controlled Key in all versions up to, and including, 2.96.6. This is due to missing ownership verification in the REST API routes registered via <code>Mappress_Api::rest_api_init()</code> , where the GET <code>/wp-json/mapp/v1/maps/{mapid}</code> endpoint uses <code>'permission_callback' => '__return_true'</code> and the write endpoints (POST update, DELETE, PATCH mutate, POST clone, POST empty_trash) only check the generic <code>'edit_posts'</code> capability without confirming that the requester owns the targeted map - a gap that is not compensated at the model layer, as <code>Mappress_Map::get()</code> , <code>'save()'</code> , <code>'delete()'</code> , <code>'mutate()'</code> , and <code>'empty_trash()'</code> all operate on any caller-supplied map ID without an ownership check. This makes it possible for unauthenticated attackers to read sensitive map data - including POI titles, addresses, coordinates, and body content - for any map on the site by enumerating map IDs, and for authenticated attackers with Contributor-level access and above to modify, delete, trash/restore, or clone any map regardless of its author.	2026-06-06	5.3	CVE-2026-8839
cifi--SEO Plugin by Squirrly SEO	The SEO Plugin by Squirrly SEO plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 12.4.16. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to invoke privileged state-changing Squirrly cloud API operations, such as revoking the site's Google Search Console and Google Analytics integrations via <code>'api/gsc/revoke'</code> and <code>'api/ga/revoke'</code> , that are otherwise restricted to administrator-level users holding the <code>'sq_manage_settings'</code> capability.	2026-06-06	4.3	CVE-2026-7624
Cisco--Cisco Finesse	A vulnerability in Cisco Finesse could allow an unauthenticated, remote attacker to load arbitrary files from remote locations into an active user session on an affected device, possibly leading to browser-based attacks. This vulnerability is due to insufficient validation of user-supplied input for HTTP requests that are sent to an affected device. An attacker who has knowledge of the address of the affected device could exploit this vulnerability by persuading a user to click a crafted link that contains the affected device address. A successful exploit could allow the attacker to conduct browser-based attacks and execute arbitrary script code in the context of the affected interface or access sensitive information on the affected device.	2026-06-03	6.1	CVE-2026-20175
Cisco--Cisco Webex Meetings	A vulnerability in the web-based user interface of Cisco Webex Meetings could have allowed an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack. Cisco has addressed this vulnerability in the Webex Meetings service, and no customer action is needed. This vulnerability existed because of insufficient validation of user input. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by persuading a user to follow a malicious link. A successful	2026-06-03	6.1	CVE-2026-20233

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploit could have allowed the attacker to execute arbitrary script code in the browser of the targeted user or access sensitive, browser-based information.			
Cloud Foundry Foundation-- windows-utilities-release	Weak Randomness / Insecure Cryptographic Primitive (CWE-338) in Get-RandomPassword in BOSH-Ecosystem / windows-utilities-release allows a network attacker to estimate VM boot time and reconstruct a small candidate list to recover the Administrator password. The randomize_password job exists solely to lock the local Administrator account behind an unguessable password as a hardening control. Because the password is derived from a predictable, clock-seeded PRNG, a network attacker who can estimate VM boot time can reconstruct a small candidate list and recover the Administrator password, defeating the hardening control. Affected versions: - windows-utilities-release: all versions prior to v0.23.0 (inclusive); fixed in v0.23.0 or later	2026-06-04	6.5	CVE-2026-41858
CloudburstMC-- Protocol	CloudburstMC Protocol is a protocol library for Minecraft Bedrock Edition. Prior to version 3.0.0.Beta12-20260420.182526-15, CloudburstMC Protocol is partially missing validation for FULL type authentication tokens (Cloudburst/Protocol). This vulnerability impacts publicly accessible software depending on the affected versions of Protocol, specifically the EncryptionUtils methods to validate auth payloads for FULL type tokens. This issue has been patched in version 3.0.0.Beta12-20260420.182526-15.	2026-06-02	5.3	CVE-2026-45289
code-projects-- Hotel and Tourism Reservation System	A security flaw has been discovered in code-projects Hotel and Tourism Reservation System 1.0. Impacted is an unknown function of the file /ht/tour.php. Performing a manipulation of the argument name /email /people /number results in cross site scripting. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	2026-06-01	4.3	CVE-2026-10289
code-projects-- Online Hospital Management System	A vulnerability has been found in code-projects Online Hospital Management System 1.0. Affected is an unknown function of the file appointmentdetail.php of the component Appointment Handler. The manipulation of the argument editid leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.	2026-06-01	6.3	CVE-2026-10209
CodeAstro-- Ingredients Stock Management System	A flaw has been found in CodeAstro Ingredients Stock Management System 1.0. This vulnerability affects unknown code of the file /Ingredients-Stock/stock_manager.php. This manipulation of the argument txt_search_category causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	2026-06-01	6.3	CVE-2026-10235
CodeAstro-- Payroll System	A vulnerability was found in CodeAstro Payroll System 1.0. This affects an unknown part of the file /home_employee.php. The manipulation of the argument emp_id results in sql injection. The attack may be performed from remote. The exploit has been made public and could be used.	2026-06-01	6.3	CVE-2026-10286
crafiium-- OptinCraft Drag & Drop Optins & Popup Builder for WordPress	The OptinCraft - Drag & Drop Optins & Popup Builder for WordPress plugin for WordPress is vulnerable to generic SQL Injection via the 'order_by' parameter in all versions up to, and including, 1.2.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional	2026-06-06	4.9	CVE-2026-8978

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	SQL queries into already existing queries that can be used to extract sensitive information from the database.			
D-Link--DWR-M920	A vulnerability was detected in D-Link DWR-M920 1.1.50/1.1.70. Affected is the function sub_41C8E8 of the file /boafm/formSmsManage. Performing a manipulation of the argument action_value results in command injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	2026-06-05	6.3	CVE-2026-10878
D-Link--DWR-M920	A vulnerability was detected in D-Link DWR-M920 up to 1.1.50. The affected element is the function sub_41CF20 of the file /boafm/formUSSDSetup. The manipulation of the argument ussdValue results in command injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	2026-06-05	6.3	CVE-2026-11339
D-Link--DWR-M920	A flaw has been found in D-Link DWR-M920 up to 1.1.50. The impacted element is the function sub_412DA0 of the file /boafm/formIMEISetup. This manipulation of the argument IMEI_value causes os command injection. The attack can be initiated remotely. The exploit has been published and may be used.	2026-06-05	6.3	CVE-2026-11341
danny-avila--LibreChat	LibreChat is an enhanced ChatGPT clone that supports multiple AI providers. In versions up to and including 0.8.3, users with only 'VIEW' access to an MCP server can retrieve the server's decrypted admin-managed secrets through 'GET /api/mcp/servers' and 'GET /api/mcp/servers/:serverName'. The returned config includes plaintext values for 'apiKey.key' and 'oauth.client_secret'. This allows viewers of a shared MCP server to exfiltrate the underlying provider credentials. Version 0.8..4 contains a patch. Other remediations include: never returning decrypted admin-managed secrets to non-owners; redacting apiKey.key and oauth.client_secret from all API responses consider returning only boolean presence indicators for secrets, similar to the auth-values route pattern; and, if owners need to edit configs without re-entering secrets, preserving secrets server-side and returning placeholders instead of plaintext.	2026-06-02	6.5	CVE-2026-44653
davidfcarr--Quick Playground	The Quick Playground plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.3.4. This is due to the 'qckply_data()' function passing the user-supplied 'filename' POST parameter directly to 'file_get_contents()' without any validation, sanitization, or path restriction. This makes it possible for authenticated attackers, with Administrator-level access and above, to read arbitrary files on the server, such as 'wp-config.php' or '/etc/passwd', which can contain sensitive information. Note: This vulnerability is only exploitable when the site has been synced with WordPress Playground (the 'is_qckply_clone' option is set) or when running on 'playground.wordpress.net'.	2026-06-06	4.4	CVE-2026-2500
ddd2500--Google Plus One Bottom	The Google Plus One Bottom plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.0.2. This is due to missing or incorrect nonce validation on the googlePlusOneAdmin function. This makes it possible for unauthenticated attackers to modify the plugin's settings, including the plusone-lang, plusone-callback, and plusone-url options stored in the database via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-02	4.3	CVE-2026-9723

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
decolua--9router	A security vulnerability has been detected in decolua 9router up to 0.4.0. This issue affects the function isAuthenticated of the file src/dashboardGuard.js of the component HTTP Header Handler. The manipulation of the argument Host leads to improper authorization. The attack is possible to be carried out remotely. Upgrading to version 0.4.1 is capable of addressing this issue. The identifier of the patch is 428e2c045cb9c0eb8080e8b580471a9c2eaa95ca. Upgrading the affected component is recommended.	2026-06-01	6.3	CVE-2026-10269
decompress--decompress	All versions of the package decompress are vulnerable to Arbitrary File Write via Archive Extraction (Zip Slip) when extracting a ZIP archive containing two entries with the same path - the first being a symlink to an arbitrary target and the second being a regular file - the file content is written through the symlink to the target location outside the output directory. This is due to the microtask processing order that checks readlink for the second file before resolving symlink for the first file. An attacker can write arbitrary file on the host filesystem potentially leading to remote code execution by providing a specially crafted ZIP archive. **Note:** This bypasses all existing path traversal protections including preventWritingThroughSymlink, added as a part of the fix for [CVE-2020-12265](https://security.snyk.io/vuln/SNYK-JS-DECOMPRESS-557358).	2026-06-05	6.4	CVE-2026-10732
DedeCMS--DedeCMS	A flaw has been found in DedeCMS 5.7.88. Affected by this vulnerability is the function base64_decode of the file /plus/download.php?open=1. This manipulation of the argument Link causes server-side request forgery. Remote exploitation of the attack is possible. The exploit has been published and may be used.	2026-06-02	6.3	CVE-2026-10581
DeepAI--api.deepai.org	The DeepAI endpoint 'https://api.deepai.org/change_user_email' accepts POST requests without any CSRF protection. If an attacker can trick a logged-in user into clicking a malicious link, the attacker can change the user's email address and take over their account. Fixed on 2026-05-20.	2026-06-01	5	CVE-2026-49433
Dell--ThinOS 10	Dell ThinOS 10, versions prior to ThinOS10 2602_10.0765, contain an Improper Access control vulnerability. An unauthenticated attacker with physical access could potentially exploit this vulnerability, leading to Information exposure.	2026-06-02	6.1	CVE-2026-40713
den-media--hiWeb Migration Simple	The hiWeb Migration Simple plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'new_domain' parameter in all versions up to, and including, 2.0.0.1 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick an administrator into performing an action such as clicking on a link.	2026-06-02	6.1	CVE-2026-2425
DevaslanPHP--project-management	A flaw has been found in DevaslanPHP project-management up to 2.0.0-beta1. Affected by this vulnerability is the function editComment/doDeleteComment of the file app/Filament/Resources/TicketResource/Pages/ViewTicket.php of the component Livewire Handler. Executing a manipulation can lead to improper authorization. The attack can be executed remotely. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	5.4	CVE-2026-10284

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
DevaslanPHP--project-management	A vulnerability has been found in DevaslanPHP project-management up to 2.0.0-beta1. Affected by this issue is the function KanbanScrumHelper::recordUpdated of the file app/Helpers/KanbanScrumHelper.php of the component Ticket Handler. The manipulation leads to improper authorization. The attack is possible to be carried out remotely. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	5.4	CVE-2026-10285
dfir-iris--iris-web	IRIS is a web collaborative platform that helps incident responders share technical details during investigations. Versions prior to 2.4.28 do not properly validate uploaded files. The application can therefore be misused to host phishing pages, amongst other things. This also creates another instance of a Cross-Site Scripting (XSS) vulnerability. Version 2.4.28 contains a patch.	2026-06-04	6.3	CVE-2026-42538
dfir-iris--iris-web	IRIS is a web collaborative platform that helps incident responders share technical details during investigations. Versions prior to 2.4.28 return sensitive data to the user which are not required for the client's operation. Version 2.4.28 contains a patch.	2026-06-04	6.5	CVE-2026-42539
dfir-iris--iris-web	IRIS is a web collaborative platform that helps incident responders share technical details during investigations. In versions prior to 2.4.28, users can create alerts for customers that are not assigned to them. This can be abused to falsely attribute fake alerts to customers. In combination with Cross-Site Scripting, this can also be used to exfiltrate alerts from other customers. Version 2.4.28 contains a patch.	2026-06-04	5.4	CVE-2026-42547
dfir-iris--iris-web	Iris is a web collaborative platform that helps incident responders share technical details during investigations. Versions prior to 2.4.28 contain a weakness where an attacker can misuse it to redirect the user to a malicious website controlled by an attacker. Version 2.4.28 fixes the issue.	2026-06-04	4.7	CVE-2026-42329
dfir-iris--iris-web	IRIS is a web collaborative platform that helps incident responders share technical details during investigations. Versions prior to 2.4.28 allow a user to alter values in the database via manipulated API requests. Version 2.4.28 contains a patch.	2026-06-04	4.3	CVE-2026-42540
dfir-iris--iris-web	IRIS is a web collaborative platform that helps incident responders share technical details during investigations. Versions prior to 2.4.28 are vulnerable to a cross-site request forgery attack, because they use the HTTP method `GET` to change state on the server. Version 2.4.28 contains a patch.	2026-06-04	4.3	CVE-2026-42543
Ditec a.s.--D.Launcher 2	D.Launcher 2 component of Slovak eID client ecosystem contains Improper URL Handler Processing vulnerability. Application registers multiple custom URL handlers that could be exploited to initiate full NTLM authentication or SMB connection to attacker infrastructure and to conduct SSRF (Server Side Request Forgery) attacks. User interaction is required as potential victim needs to open a specially crafted URL.	2026-06-02	6.5	CVE-2026-8993
djangoproject--daphne	daphne before 4.2.2 did not pass maxFramePayloadSize or maxMessagePayloadSize to Autobahn's WebSocketServerFactory. Because Autobahn defaults both values to 0 (unlimited), an unauthenticated remote attacker could send arbitrarily large WebSocket messages or frames, causing excessive memory consumption and a denial of service.	2026-06-03	5.3	CVE-2026-44545

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dolibarr--ERP CRM	A security vulnerability has been detected in Dolibarr ERP CRM up to 23.0.1. Impacted is the function checkUserAccessToObject of the file htdocs/holiday/class/api_holidays.class.php of the component Leave Request REST API. The manipulation leads to improper authorization. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 23.0.2 is recommended to address this issue. The identifier of the patch is ee93b6f2f9dd0f6aeefe9d718ab3ab0a44326b73. Upgrading the affected component is advised.	2026-06-01	4.3	CVE-2026-10215
Dräger--Atlan A350	Dräger Atlan A350 software versions 1.00 through 1.01 contains an improper input handling vulnerability that allows attackers to cause a denial of service by sending specifically crafted non-Medibus-compliant data through the Medibus interface. Attackers can transmit malformed data to overload the internal processor, gradually disrupting device operation over several hours and causing loss of data transmission, delayed display of real-time curves, and deviation between displayed airway pressure values and screen curves.	2026-06-02	4	CVE-2021-4479
Dräger--Infinity Delta	Dräger Infinity Delta, Delta XL, and Kappa patient monitors contain a denial-of-service vulnerability that allows remote attackers to cause the monitor to reboot by sending a malformed network packet. Attackers can repeatedly send malformed network packets to disrupt patient monitoring until the device falls back to default configuration and loses network connectivity.	2026-06-01	6.5	CVE-2019-25716
Dräger--Infinity Delta	Dräger Infinity Delta, Delta XL, and Kappa patient monitors contain an information disclosure vulnerability that allows unauthenticated network attackers to access log files over a network connection. Attackers can retrieve device internals, location information, and wired network configuration details from the exposed log files.	2026-06-02	4.3	CVE-2019-25717
Dräger--Infinity M300	Dräger Infinity M300 patient worn monitors with software version VG2.3.1 and earlier contain a network-based denial of service vulnerability that allows network-adjacent attackers to repeatedly trigger device reboots by sending malicious requests over the Infinity Network. Attackers can exploit this vulnerability to force the device into a fail state requiring manual restart, causing loss of wireless connectivity and interruption of patient monitoring functionality.	2026-06-02	6.5	CVE-2019-25721
Dräger--Infinity M300	Dräger Infinity M300 patient worn monitors with software version VG2.x and earlier contain a network-based denial of service vulnerability that allows attackers with access to the hospital or Infinity Network to repeatedly trigger device reboots until the device enters a fail state requiring manual restart. Attackers can exploit this vulnerability to cause loss of wireless network connectivity, temporary loss of patient monitoring, and interruption of alarm functionality until the device is manually recovered.	2026-06-02	6.5	CVE-2019-25724
Dräger--Perseus A500	Dräger Perseus A500 software versions 2.00 through 2.02 contains an improper input handling vulnerability that allows external attackers to cause a denial of service by sending specifically crafted non-Medibus-compliant data through the Medibus interface. Attackers can overload the internal processor with malformed data to trigger a warm restart, causing	2026-06-02	4	CVE-2019-25723

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ventilation pressure to drop to ambient level and interrupting ventilation for several seconds before therapy resumes.			
Dräger--SC 6002XL	Dräger SC Monitoring devices (SC 6002XL, SC 6802XL, SC 7000, SC 8000, SC 9000 XL) contain a denial-of-service vulnerability in all software versions that allows unauthenticated attackers to reboot the monitor by sending a malformed network packet. Attackers can repeatedly send such malformed packets to disrupt patient monitoring until the device falls back to default configuration and loses network connectivity.	2026-06-03	6.5	CVE-2019-25720
Dräger--Zeus IE	Dräger Zeus Infinity Empowered (Zeus IE) and Zeus RS C500 anesthesia workstations contain a local security vulnerability that allows unauthorized individuals with physical access to compromise software integrity via USB interface manipulation. Attackers can exploit the unprotected USB interfaces to impair therapy functions, manipulate device-processed data, or leverage the device as a pivot point for broader network-based attacks when connected to a network or Dräger Service Connect.	2026-06-02	6.8	CVE-2025-15653
EIPStackGroup--OpENER	A security vulnerability has been detected in EIPStackGroup OpENER up to 2.3.0. Affected is the function CreateMessageRouterRequestStructure of the file cipmessengerouter.c of the component SendRRData Handler. The manipulation leads to use after free. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-03	6.3	CVE-2026-10703
elabftw--elabftw	eLabFTW is an open source electronic lab notebook. Prior to version 5.4.2, in certain cases, an authenticated user performing a numeric reference/search can return results that include resources the requesting user is not authorized to view. The exposed information is limited (only the title). Attempts to access the underlying protected resource content remain blocked by authorization checks. Version 5.4.2 fixes the issue. # Affected Scope Cross-scope visibility of titles. No confirmed bypass of content-level access controls # Preconditions An authenticated user account No special privileges required beyond standard access # Impact This may enable unauthorized disclosure of sensitive information if confidential data is included in resource titles. Examples could include project names, patient identifiers, or other regulated information embedded in titles.	2026-06-01	4.3	CVE-2026-28511
Elementor--Elementor Website Builder	Missing Authorization vulnerability in Elementor Elementor Website Builder allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Elementor Website Builder: from n/a through 4.1.0.	2026-06-02	5.4	CVE-2026-49782
elunez--eladmin	A weakness has been identified in elunez eladmin up to 2.7. This vulnerability affects unknown code of the file App.java of the component Application Deployment Module. This manipulation of the argument uploadPath causes command injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-02	6.3	CVE-2026-10550

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Emilia Projects--Progress Planner	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Emilia Projects Progress Planner allows Stored XSS. This issue affects Progress Planner: from n/a through 1.9.0.	2026-06-02	5.9	CVE-2026-28116
Enderfga--claw-orchestrator	A security vulnerability has been detected in Enderfga claw-orchestrator up to 3.7.0. The impacted element is the function validateRegex of the file claw-orchestrator/src/embedded-server.ts of the component Session Grep Endpoint. The manipulation of the argument body.pattern leads to inefficient regular expression complexity. The attack may be initiated remotely. Upgrading to version 3.7.1 is sufficient to resolve this issue. The identifier of the patch is 3f970a974c65a94555c25af9f2796f11315e4584. It is recommended to upgrade the affected component.	2026-06-01	4.3	CVE-2026-10291
epoupon--lms	Lightweight Music Server (LMS) though 3.76.0 contains a stored cross-site scripting vulnerability that allows attackers to execute arbitrary JavaScript by embedding malicious HTML in media file metadata tags such as GENRE, ARTIST, or ALBUM. Attackers can introduce a crafted media file into the victim's library, causing the payload to be saved during library scanning and executed automatically in the web interface due to tag content being rendered using Wt::TextFormat::UnsafeXHTML without sanitization in src/lms/ui/Utils.cpp.	2026-06-01	5.4	CVE-2026-48559
Ericsson--Packet Core Controller	Ericsson Packet Core Controller (PCC) versions prior to 1.39 contain a vulnerability where an attacker sending a large volume of specially crafted messages may cause service degradation.	2026-06-05	6.5	CVE-2025-59174
erzhongxmu--JeeWMS	A weakness has been identified in erzhongxmu JeeWMS up to 141740afb2ba14d441c82a833d0a418d07ca2d69. This issue affects some unknown processing of the file /base-boot/actuator of the component Boot Actuator Endpoint. Executing a manipulation can lead to information disclosure. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-07	5.3	CVE-2026-11458
expresstech--Quiz and Survey Master (QSM) Easy Quiz and Survey Maker	The Quiz and Survey Master (QSM) - Easy Quiz and Survey Maker plugin for WordPress is vulnerable to time-based blind SQL Injection via the 'order' parameter in all versions up to, and including, 11.1.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with admin-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. If the secret key is exposed, this can be exploited by lower-privileged users.	2026-06-05	4.9	CVE-2026-6448
federicocarrara--rognone	The rognone plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'mode' parameter in versions up to, and including, 0.6.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2026-06-02	6.1	CVE-2026-1450
federicocarrara--rognone	The rognone plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'a' parameter in versions up to, and including, 0.6.2 due to insufficient input sanitization and output escaping. This makes it possible	2026-06-02	6.1	CVE-2026-1451

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.			
flippercode--WP Maps Google Maps,OpenStreetMap,Mapbox,Store Locator,Listing,Directory & Filters	The WP Maps - Google Maps,OpenStreetMap,Mapbox,Store Locator,Listing,Directory & Filters plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'location_messages' parameter in all versions up to, and including, 4.9.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Exploitation requires the attacker to hold the custom wpgmp_manage_location capability, which is granted to administrators by default but can be assigned to lower-privileged roles via the plugin's Permissions screen.	2026-06-06	4.4	CVE-2026-9594
FoundationAgents--MetaGPT	A weakness has been identified in FoundationAgents MetaGPT up to 0.8.2. This affects the function Message.check_instruct_content of the file metagpt/schema.py. Executing a manipulation of the argument mapping can lead to deserialization. The attack is restricted to local execution. The exploit has been made available to the public and could be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-02	5.3	CVE-2026-10566
FoundationAgents--MetaGPT	A vulnerability was determined in FoundationAgents MetaGPT up to 0.8.2. Affected by this issue is the function check_cmd_exists of the file metagpt/utlis/common.py. This manipulation of the argument mermaid.path causes command injection. The attack may be initiated remotely. A high degree of complexity is needed for the attack. The exploitation is known to be difficult. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-07	5	CVE-2026-11455
frankpw--FPW Category Thumbnails	The FPW Category Thumbnails plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter of the 'fpw_fs_get_file' AJAX action in all versions up to, and including, 1.9.5. This is due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever an administrator accesses the plugin's settings page.	2026-06-02	6.4	CVE-2026-2382
Fruitfulcode--Zoner Real Estate	WordPress Theme Zoner Real Estate 4.1.1 contains a persistent cross-site scripting vulnerability that allows authenticated agents to inject malicious scripts through the Address input field when creating properties. Attackers can inject JavaScript payloads in the property creation form that execute when administrators view the property for approval, enabling cookie theft and session hijacking.	2026-06-04	6.4	CVE-2019-25742
Gigtodoscript--GigToDo	GigToDo 1.3 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject malicious JavaScript and HTML code through the proposal description field. Attackers can craft XSS payloads in the create_proposal endpoint that execute when administrators or other users view the stored proposal, enabling cookie theft and malicious redirects.	2026-06-04	6.4	CVE-2019-25739

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Gitlabw--openclaude	OpenClaude is an open-source coding-agent command line interface for cloud and local model providers. Prior to version 0.5.1, the OpenClaude MCP authentication flow starts a temporary local HTTP server to handle OAuth callbacks. To prevent CSRF attacks, the server validates a state parameter against an internally stored value. However, due to a logic flaw in the order of conditionals, an attacker can completely bypass this check and force the server to shut down - without knowing the state value at all. This issue has been patched in version 0.5.1.	2026-06-02	6.5	CVE-2026-42073
GL.iNet--GL-MT3000	A security flaw has been discovered in GL.iNet GL-MT3000 up to 4.4.5. Impacted is the function iwinfo_backend of the file iwinfo.so of the component MTK Backend. The manipulation of the argument device results in command injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 4.7 is recommended to address this issue. Upgrading the affected component is recommended. The vendor confirms: "Starting from version 4.7, SDK has added global protection to intercept malicious injection".	2026-06-07	6.3	CVE-2026-11447
GL.iNet--GL-MT3000	A security vulnerability has been detected in GL.iNet GL-MT3000 4.4.5. The impacted element is the function rpc_sys of the file /cgi-bin/luci/rpc of the component LuCI JSON-RPC Interface. Such manipulation leads to command injection. The attack may be performed from remote. Upgrading to version 4.8.1 is sufficient to resolve this issue. Upgrading the affected component is advised. The vendor confirms: "The issue discovered by the vulnerability researcher on older firmware versions(4.4.5) has actually been fixed and mitigated in the new version. According to the latest firmware fixes, by default, firmware versions after 4.7.13 do not install LuCI, so this vulnerability cannot be exploited."	2026-06-07	6.3	CVE-2026-11449
GL.iNet--GL-MT3000	A weakness has been identified in GL.iNet GL-MT3000 up to 4.4.5. The affected element is the function realpath of the file /rpc of the component Minidlna Service. This manipulation of the argument kube. set causes command injection. The attack is possible to be carried out remotely. Upgrading to version 4.7 is sufficient to fix this issue. It is recommended to upgrade the affected component. The vendor confirms: "Starting from version 4.7, SDK has added global protection to intercept malicious injection".	2026-06-07	4.7	CVE-2026-11448
GL.iNet--MT3000	A vulnerability was determined in GL.iNet MT3000 up to 4.4.5. This vulnerability affects unknown code of the file ovpnclient.sh of the component OpenVPN Client Import Workflow. This manipulation causes command injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. Upgrading to version 4.9.0_beta3-1012-0513-1778656146 is able to resolve this issue. You should upgrade the affected component. The vendor confirms: "This issue has been addressed by implementing malicious checks on OpenVPN configuration files to prevent command injection attacks carried through malicious configuration files."	2026-06-06	6.3	CVE-2026-11406
glenwpcoder--Drag and Drop Multiple File	The Drag and Drop Multiple File Upload for Contact Form 7 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'drag_n_drop_text' and 'drag_n_drop_browse_text' Settings in all versions up to, and including, 1.3.9.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with	2026-06-06	4.4	CVE-2026-8991

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Upload for Contact Form 7	administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
go-git--go-billy	Billy is an interface filesystem abstraction for Go. Prior to versions 5.9.0 and 6.0.0-alpha.1, multiple components may improperly handle crafted or malformed input, resulting in panics, infinite loops, uncontrolled recursion, or excessive resource consumption. These issues arise from insufficient validation and missing safety mechanisms such as cycle detection, recursion limits, or defensive handling of unexpected states when processing untrusted repository data and filesystem structures. This issue has been patched in versions 5.9.0 and 6.0.0-alpha.1.	2026-06-01	6.5	CVE-2026-44740
haxtheweb--haxcms-nodejs	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Prior to version 26.0.0, the HAX CMS NodeJS application crashes when an authenticated attacker sends a specially crafted site creation request to the createSite endpoint. A single request is sufficient to take the entire application offline, requiring a manual server restart to restore service. Version 26.0.0 fixes the issue.	2026-06-05	6.5	CVE-2026-46357
haxtheweb--haxcms-php	HAX CMS helps manage microsite universe with PHP or NodeJs backends. Prior to version 26.0.0, an Authenticated Local File Inclusion (LFI) vulnerability in the HAXCMS saveOutline endpoint allows a low-privileged user to read arbitrary files on the server by manipulating the location field written into site.json. This enables attackers to exfiltrate sensitive system files such as /etc/passwd, application secrets, or configuration files accessible to the web server (www-data). Version 26.0.0 patches the issue.	2026-06-05	6.5	CVE-2026-46397
HCL--iControl	HCL iControl was affected by Weak Input Validation vulnerability. This weakness is caused during implementation of an architectural security tactic. Received input that is expected to be of a certain type, but it does not validate or incorrectly validates that the input is actually of the expected type.	2026-06-04	4.3	CVE-2025-52606
HCLSoftware--Digital Experience & DX Compose	HCL Digital Experience and HCL Digital Experience Compose could be susceptible to Host header injection. An attacker can manipulate the Host header and cause the application to behave in unexpected ways.	2026-06-05	6.1	CVE-2026-21826
HCLSoftware--DX Compose	HCL Digital Experience Compose is affected by a reflected cross-site scripting (XSS) vulnerability in the search center. An attacker could execute arbitrary JavaScript in the victim's browser.	2026-06-05	6.1	CVE-2026-21825
hekmon8--Jenkins-server-mcp	A vulnerability has been found in hekmon8 Jenkins-server-mcp 0.1.0. This vulnerability affects the function jobPath of the file src/index.ts of the component get_build_status/get_build_log/trigger_build. Such manipulation leads to server-side request forgery. The attack may be performed from remote. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	6.3	CVE-2026-10276
HelloTalk--HelloTalk	HelloTalk through 3.4.1 stores full-precision GPS coordinates even when the user had intended to share only a country or city. Furthermore, these coordinates are placed into a database on the client of other users. (The client side was changed in 2019 to encrypt that database.)	2026-06-05	5.3	CVE-2020-25900

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hiraishikentaro--wezterm-mcp	A vulnerability was identified in hiraishikentaro wezterm-mcp 0.1.0. The affected element is an unknown function of the file src/wezterm_executor.ts of the component switch_pane/write_to_specific_pane. The manipulation of the argument request.params.arguments.pane_id leads to os command injection. The attack can be initiated remotely. The exploit is publicly available and might be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	6.3	CVE-2026-10279
HKUDS--nanobot	Nanobot prior to version 0.2.1 contains a server-side request forgery vulnerability in the web_fetch tool that allows remote attackers to reach internal or private network hosts by supplying a URL that redirects to a loopback or private address via a 3xx Location header. Attackers can exploit the automatic HTTP redirect following behavior in the httpx library to bypass initial URL validation and cause the runtime to send outbound requests to internal hosts before final resolved URL validation is applied.	2026-06-01	5	CVE-2026-49138
HKUDS--nanobot	Nanobot prior to version 0.2.1 contains a denial of service vulnerability in the Matrix channel media download handler that allows authenticated room members to exhaust process memory and bandwidth by sending media events with missing or invalid size metadata. Attackers can send multiple concurrent Matrix media events with omitted or invalid declared sizes to trigger simultaneous large media downloads that fully materialize response bodies before post-download rejection, consuming process resources until service degradation occurs.	2026-06-01	4.3	CVE-2026-49140
holithemes--Click to Chat HoliThemes	The Click to Chat - WA Widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the [chat] shortcode 'num' parameter in all versions up to, and including, 4.38. This is due to insufficient escaping when embedding user-supplied shortcode attribute values inside JavaScript string literals that are then placed in HTML event-handler attributes. The CCW_Shortcode::shortcode() function applies esc_attr() to the 'num' parameter (line 157), which converts single quotes to the HTML entity '. This entity-encoded value is then interpolated directly into a JavaScript window.open() call string delimited by single quotes (line 194/221), and that complete string is placed verbatim into an HTML onclick attribute in the style template files (e.g., sc-style-1.php line 6). Because browsers HTML-decode event attribute values before executing the embedded JavaScript, the ' entities are decoded back to literal single quotes at runtime, allowing the injected payload to break out of the JavaScript string context and execute arbitrary code. This makes it possible for authenticated attackers with Contributor-level access and above to inject arbitrary web scripts into pages that will execute whenever a user clicks the WhatsApp chat button rendered by the [chat] shortcode.	2026-06-06	6.4	CVE-2026-7795
iAI Lab--PDF AI App	A security flaw has been discovered in iAI Lab PDF AI App 4.21.0 on Android. Impacted is the function getExternalCacheDir of the component chatpdf.pro. Performing a manipulation of the argument _display_name results in path traversal. The attack requires a local approach. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-06	4.4	CVE-2026-11411

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
indrasishbanerjee--aem-mcp-server	A vulnerability was determined in indrasishbanerjee aem-mcp-server up to b5f833aef9b5dfd17a5991b3b18a8a11eddbc583. This impacts the function getAssetMetadata of the file src/mcp-server.ts of the component Axios Request Flow. Executing a manipulation of the argument assetPath can lead to server-side request forgery. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	6.3	CVE-2026-10274
ishayoyo--excel-mcp	A vulnerability was determined in ishayoyo excel-mcp up to 1.0.2. Impacted is an unknown function of the file src/index.ts of the component read_file/write_file. Executing a manipulation of the argument filePath/outputPath can lead to path traversal. It is possible to launch the attack remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	6.3	CVE-2026-10278
ITPison--OMICARD EDM	OMICARD EDM developed by ITPison has a Insecure Direct Object Reference vulnerability, allowing unauthenticated remote attackers to modify a specific parameter to obtain user's email address.	2026-06-04	5.3	CVE-2026-10597
itsourcecode--Content Management System	A weakness has been identified in itsourcecode Content Management System 1.0. This impacts an unknown function of the file /instructions.php. This manipulation of the argument topic_id causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	2026-06-01	6.3	CVE-2026-10242
itsourcecode--Content Management System	A vulnerability was identified in itsourcecode Content Management System 1.0. This vulnerability affects unknown code of the file /save_comment.php. The manipulation of the argument Name leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	2026-06-01	6.3	CVE-2026-10256
itsourcecode--Content Management System	A security flaw has been discovered in itsourcecode Content Management System 1.0. This issue affects some unknown processing of the file /admin/update_ss_img.php. The manipulation of the argument topic_id results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	2026-06-01	6.3	CVE-2026-10257
itsourcecode--Content Management System	A weakness has been identified in itsourcecode Content Management System 1.0. Impacted is an unknown function of the file /admin/add_sub_topic.php. This manipulation of the argument topic_id causes sql injection. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	2026-06-01	6.3	CVE-2026-10258
itsourcecode--Content Management System	A vulnerability was identified in itsourcecode Content Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/edit_topic.php. Such manipulation of the argument topic_id leads to sql injection. The attack may be launched remotely. The exploit is publicly available and might be used.	2026-06-01	6.3	CVE-2026-10265
itsourcecode--Fees	A vulnerability was determined in itsourcecode Fees Management System 1.0. Affected by this issue is some unknown functionality of the file /ajax.php. Executing a manipulation of the argument Username can lead	2026-06-01	6.3	CVE-2026-10296

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	to sql injection. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized.			
itsourcecode-- Fees Management System	A vulnerability was identified in itsourcecode Fees Management System 1.0. This affects an unknown part of the file /manage_course.php. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit is publicly available and might be used.	2026-06-01	6.3	CVE-2026-10297
itsourcecode-- Fees Management System	A flaw has been found in itsourcecode Fees Management System 1.0. The impacted element is an unknown function of the file /manage_fee.php. Executing a manipulation of the argument ID can lead to sql injection. The attack may be launched remotely. The exploit has been published and may be used.	2026-06-01	6.3	CVE-2026-10302
itsourcecode-- Fees Management System	A vulnerability was detected in itsourcecode Fees Management System 1.0. Affected is an unknown function of the file /manage_payment.php. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	2026-06-02	6.3	CVE-2026-10568
itsourcecode-- Fees Management System	A vulnerability was identified in itsourcecode Fees Management System 1.0. This affects an unknown function of the file /manage_student.php. The manipulation of the argument ID leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	2026-06-04	6.3	CVE-2026-10808
itsourcecode-- Fees Management System	A security flaw has been discovered in itsourcecode Fees Management System 1.0. This impacts an unknown function of the file /manage_user.php. The manipulation of the argument ID results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	2026-06-04	6.3	CVE-2026-10809
itsourcecode-- Fees Management System	A security vulnerability has been detected in itsourcecode Fees Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /receipt.php. Such manipulation of the argument ef_id leads to sql injection. The attack may be performed from remote. The exploit has been disclosed publicly and may be used.	2026-06-04	6.3	CVE-2026-10811
itsourcecode-- Fees Management System	A vulnerability was detected in itsourcecode Fees Management System 1.0. The affected element is an unknown function of the file index.php. Performing a manipulation of the argument page results in cross site scripting. The attack may be initiated remotely. The exploit is now public and may be used.	2026-06-01	4.3	CVE-2026-10301
itsourcecode-- Fees Management System	A weakness has been identified in itsourcecode Fees Management System up to 1.0. Affected is an unknown function of the file /navbar.php. This manipulation of the argument page causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been made available to the public and could be used for attacks.	2026-06-04	4.3	CVE-2026-10810
j3k0--mcp-google-workspace	A vulnerability was found in j3k0 mcp-google-workspace up to 831790e7d5c2663325733d9f5579cc339a267c4c. This issue affects the function saveToDisk of the file src/tools/gmail.ts of the component MCP Gmail Tool. Performing a manipulation results in improper access controls. It is possible to initiate the attack remotely. The exploit has been made public and could be used. This product is using a rolling release to provide	2026-06-01	6.3	CVE-2026-10277

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	continious delivery. Therefore, no version details for affected nor updated releases are available. The patch is named 89c091ecf8b9f9c7291d1af0b1966e271f86551c. It is suggested to install a patch to address this issue.			
jamesmuga--Remove NoFollow Commenter URL	The Remove NoFollow Commenter URL plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0. This is due to missing or incorrect nonce validation on the gmz_comment_settings_save function. This makes it possible for unauthenticated attackers to modify the plugin's comment-display setting via a forged request via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-02	4.3	CVE-2026-9730
JeecgBoot--JeecgBoot	A vulnerability was determined in JeecgBoot up to 3.9.2. The affected element is the function WordUtil.addImage of the file /airag/word/edit. Executing a manipulation can lead to server-side request forgery. The attack can be executed remotely. The exploit has been publicly disclosed and may be utilized. A fix is planned for the upcoming release.	2026-06-01	6.3	CVE-2026-10239
JeecgBoot--JeecgBoot	A vulnerability was identified in JeecgBoot up to 3.9.2. The impacted element is an unknown function of the file /airag/airagModel/test. The manipulation of the argument baseUrl leads to server-side request forgery. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. A fix is planned for the upcoming release.	2026-06-01	6.3	CVE-2026-10240
jeecgboot--The server processes these URLs	A security flaw has been discovered in jeecgboot The server processes these URLs up to 3.9.1. This affects the function FileDownloadUtils.download2DiskFromNet of the file /airag/app/debug of the component Cloud Instance Metadata Endpoint. The manipulation results in server-side request forgery. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. Upgrading to version 3.9.2 mitigates this issue. It is suggested to upgrade the affected component.	2026-06-01	6.3	CVE-2026-10241
jhdscript--ZeM STL	The ZeM STL plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the [zemstl] shortcode in all versions up to and including 1.0. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes, specifically the 'url', 'color', and 'bgcolor' parameters. These attribute values are directly interpolated into HTML attribute context without being passed through esc_attr() or any other escaping function. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-02	6.4	CVE-2026-4081
Jinher--OA	A weakness has been identified in Jinher OA C6. The affected element is an unknown function of the file /C6/JHSoft.Web.ModuleCount/GetFormSn.aspx. Executing a manipulation of the argument queryID can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-06	6.3	CVE-2026-11412
jishenghua--jshERP	A security vulnerability has been detected in jishenghua jshERP up to 3.6. This vulnerability affects the function addAccountHeadAndDetail of the file jshERP-boot/src/main/java/com/jsh/erp/service/AccountHeadService.java of the component addAccountHeadAndDetail Endpoint. Such manipulation	2026-06-07	5.4	CVE-2026-11467

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of the argument fileName leads to path traversal. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.			
jishenghua--jshERP	A flaw has been found in jishenghua jshERP up to 3.6. Impacted is the function insertPlatformConfig of the file jshERP-boot/src/main/java/com/jsh/erp/service/PlatformConfigService.java of the component platformConfig Add Endpoint. Executing a manipulation of the argument platformValue can lead to server-side request forgery. The attack may be performed from remote. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-07	4.7	CVE-2026-11469
johnhuang316--code-index-mcp	A weakness has been identified in johnhuang316 code-index-mcp up to 2.14.0. Affected is the function is_safe_regex_pattern of the component search_code_advanced. Executing a manipulation of the argument regex can lead to inefficient regular expression complexity. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 2.14.1 is able to address this issue. This patch is called 25bc02fac74051ddae15ce79e952f00211b1ea6b. Upgrading the affected component is recommended.	2026-06-02	4.3	CVE-2026-10692
Joomsky--JS Jobs	Joomla com_jsjobs 1.2.6 contains an arbitrary file deletion vulnerability that allows authenticated attackers to delete files by manipulating custom userfield parameters. Attackers can send POST requests to the job.savejob task with path traversal sequences in the field_2 parameter to delete arbitrary files accessible to the web server.	2026-06-04	6.5	CVE-2019-25740
keystonejs--keystone	A vulnerability was detected in keystonejs keystone up to 20260319. This vulnerability affects unknown code in the library packages/core/src/lib/core/queries/output-field.ts of the component GraphQL API Endpoint. The manipulation results in resource consumption. It is possible to launch the attack remotely. The exploit is now public and may be used. The pull request to fix this issue awaits acceptance.	2026-06-04	4.3	CVE-2026-10802
kiteworks--Secure Data Forms	Kiteworks is a private data network (PDN). Prior to version 9.3.0, an Insecure Direct Object Reference (IDOR) vulnerability in Kiteworks Secure Data Forms allows an authenticated attacker to tamper with the internal approval flow configurations of forms belonging to other users due to insufficient authorization checks on resource ownership. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	2026-06-01	6.5	CVE-2026-23638
kiteworks--Secure Data Forms	Kiteworks is a private data network (PDN). Prior to version 9.3.0, an Insecure Direct Object Reference (IDOR) vulnerability in Kiteworks Secure Data Forms allows an authenticated user to modify resources belonging to other users due to insufficient authorization checks on resource ownership. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	2026-06-01	6.5	CVE-2026-24753
kiteworks--Secure Data Forms	Kiteworks is a private data network (PDN). Prior to version 9.3.0, an Insecure Direct Object Reference (IDOR) vulnerability in Kiteworks Secure Data Forms allows an authenticated user to modify permissions on resources belonging to other users due to insufficient authorization checks	2026-06-01	5.4	CVE-2026-24755

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	on resource ownership. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.			
kiteworks--Secure Data Forms	Kiteworks is a private data network (PDN). Prior to version 9.3.0, an Insecure Direct Object Reference (IDOR) vulnerability in Kiteworks Secure Data Forms allows an authenticated user to modify resources belonging to other users due to insufficient authorization checks on resource ownership. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	2026-06-01	4.3	CVE-2026-24756
kiteworks--security-advisories	Kiteworks is a private data network (PDN). Prior to version 9.3.0, a stored XSS vulnerability in Kiteworks Secure Data Forms could allow an authenticated attacker to execute arbitrary JavaScript code in other users' sessions. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	2026-06-01	5.4	CVE-2026-24754
klamra22--Klamra Paycal for Aspaclaria	The Klamra Paycal for Aspaclaria plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.1.4 via the 'invoice_id' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to download arbitrary customer invoices by enumerating sequential post IDs, exposing sensitive billing PII including full name, email address, phone number, order total, line items, and customer notes belonging to other customers.	2026-06-06	4.3	CVE-2026-8611
LakshayD02--Hostel-Management-System-PHP	A vulnerability was found in LakshayD02 Hostel-Management-System-PHP up to f87e67c283bab6f718faf2fec6ae39a13bd7036b. This issue affects some unknown processing of the file hostel/index.php of the component Admin Dashboard Page. The manipulation of the argument ID results in missing authorization. The attack can be launched remotely. The exploit has been made public and could be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-04	6.3	CVE-2026-10815
latepoint--LatePoint Calendar Booking Plugin for Appointments and Events	The LatePoint - Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.6.0. This is due to missing or incorrect nonce validation on the change_status function. This makes it possible for unauthenticated attackers to change the status of arbitrary invoices - including marking unpaid invoices as paid - without administrator consent via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-05	4.3	CVE-2026-9719
libexpat project--libexpat	libexpat before 2.8.2 lacks handler call depth tracking for calls to XML_GetBuffer, XML_Parse, XML_ParseBuffer, XML_ParserFree, or XML_ParserReset from within handlers in cases of a policy violation. Thus, a use-after-free can occur,	2026-06-04	4.9	CVE-2026-50219
litonice13--Master Addons For Elementor Widgets, Extensions, Theme Builder, Popup Builder & Template Kits	The Master Addons For Elementor - Widgets, Extensions, Theme Builder, Popup Builder & Template Kits plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'jtlma_custom_js' Page Setting (Custom JS Extension) in all versions up to, and including, 3.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The unfiltered_html capability check is only enforced during Elementor control registration (UI rendering) and not during the	2026-06-06	6.4	CVE-2026-9281

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	save process, enabling Author-level users to inject the jtlma_custom_js setting directly via a crafted POST request to admin-ajax.php?action=elementor_ajax, bypassing the UI-level restriction entirely.			
LMS Community--Lyrion Music Server	Lyrion Music Server 9.2.0 contains an unauthenticated reflected cross-site scripting vulnerability in the server.log endpoint that allows attackers to inject arbitrary HTML and JavaScript code through the search parameter. Attackers can craft malicious URLs with JavaScript payloads in the search parameter to execute code in users' browsers within the context of the affected application.	2026-06-05	6.1	CVE-2026-50230
LMS Community--Lyrion Music Server	Lyrion Music Server 9.2.0 contains a reflected cross-site scripting vulnerability in advanced search parameters that fail to properly sanitize user input before displaying it in search forms. Attackers can inject malicious scripts through unfiltered search parameters to execute arbitrary JavaScript in users' browsers and steal session information.	2026-06-05	6.1	CVE-2026-50235
LMS Community--Lyrion Music Server	Lyrion Music Server 9.2.0 contains an arbitrary directory listing vulnerability in its readdirectory query, exposed through both the CLI service (TCP port 9090) and the HTTP JSON-RPC endpoint (/jsonrpc.js). The query accepts a folder parameter and lists its contents with no restriction to the configured media directories and no authentication in the default configuration, allowing a remote, unauthenticated attacker to enumerate arbitrary locations on the host filesystem.	2026-06-05	5.3	CVE-2026-50233
Mage AI--Mage AI	A vulnerability was detected in Mage AI up to 0.9.79. This impacts the function useMutation of the file mage_ai/frontend/components/Sessions/SignForm/index.tsx of the component Sign-in Flow. Performing a manipulation of the argument query.redirect_url results in cross site scripting. Remote exploitation of the attack is possible. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-06	4.3	CVE-2026-11436
Mamunur Rashid--Classified Listing	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Mamunur Rashid Classified Listing allows Path Traversal. This issue affects Classified Listing: from n/a through 5.3.8.	2026-06-01	6.5	CVE-2026-42679
marcqueral--DeMomentSomTres Shortcodes	The DeMomentSomTres Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'callout' shortcode in all versions up to, and including, 1.1.1. This is due to insufficient input sanitization and output escaping on the 'width' and 'align' shortcode attributes within the st_callout() function, which concatenates the attribute values directly into an HTML style attribute. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-02	6.4	CVE-2026-8885
mcmilk--7-Zip	7-Zip is a file archiver with a high compression ratio. Versions 9.21 through 26.00 contain an An uninitialized memory disclosure vulnerability in the UEFI capsule (.scap) parser in 7-Zip. The OpenCapsule function allocates a heap buffer of attacker-declared CapsuleImageSize (up to 1 GiB) without zero-initialization, then reads the file contents into it with ReadStream_FALSE whose return value is silently discarded. If the file is truncated, the unread tail of the buffer retains uninitialized heap memory,	2026-06-05	6.5	CVE-2026-48101

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	which is then exposed as extracted file content via GetStream. Version 26.0.1 fixes the issue.			
mcmilk--7-Zip	7-Zip is a file archiver with a high compression ratio. Versions 9.18 through 26.00 contain a heap out-of-bounds read in 7-Zip Ar handler BSD SYMDEF parser. A 4-byte heap out-of-bounds read exists in the Unix ar archive parser in 7-Zip. When parsing a BSD-style __.SYMDEF symbol table, the ParseLibSymbols function reads a 32-bit namesSize field via Get32 at a position that can equal the buffer size, reading 4 bytes past the end of the heap allocation. This reads uninitialized heap data under the default allocator. Version 26.01 patches the issue.	2026-06-05	6.5	CVE-2026-48112
mcmilk--7-Zip	7-Zip is a file archiver with a high compression ratio. Versions 9.34 through 26.00 contain a heap memory disclosure via SquashFS fragment offset integer overflow on 32-bit builds. 32-bit integer overflow in the SquashFS ReadBlock function allows an attacker-controlled node.Offset value to bypass the fragment bounds check, causing memcpy to read heap memory preceding the cache buffer into the extracted file. The vulnerability is exploitable only on 32-bit builds of 7-Zip where size_t is 32 bits, allowing the addition offsetInBlock + blockSize to wrap modulo 2 ³² . On 64-bit builds the addition is promoted to 64 bits and the check correctly rejects the input. Version 26.01 patches the issue.	2026-06-05	4.3	CVE-2026-48092
mcmilk--7-Zip	7-Zip is a file archiver with a high compression ratio. Versions 9.34 through 26.00 contain an off-by-one heap out-of-bounds read in the WIM (Windows Imaging) archive handler's security descriptor lookup. In CHandler::GetSecurity (CPP/7zip/Archive/Wim/WimHandler.cpp), the per-image SecurOffsets table holds numEntries + 1 cumulative offsets, but the check securityId >= SecurOffsets.Size() admits securityId == numEntries, and the function then reads SecurOffsets[securityId + 1], fetching one UInt32 past the end of the heap-allocated CRecordVector (which performs no bounds checking on operator[]). The securityId is attacker-controlled at offset +0xC of any directory entry in WIM metadata, and the handler is registered for .wim, .swm, .esd, and .ppkg and enabled by default in stock 7z.dll; the OOB triggers zero-click in the GUI because 7zFM.exe's ListView calls GetRawProp(kpidNtSecure) for every item during listing (ASan-confirmed), and is also reachable via CLI listing with 7zz l -slt. Impact is limited to denial of service under hardened allocators and minor information disclosure, since the OOB value is only consumed arithmetically as a length and is not surfaced to the attacker; there is no write primitive.	2026-06-05	4.3	CVE-2026-48103
mcmilk--7-Zip	7-Zip is a file archiver with a high compression ratio. Versions 9.18 through 26.00 contain an uninitialized heap read in the SquashFS archive handler caused by a sparsely populated index array. In the SquashFS handler, _blockToNode is allocated with capacity for every metadata block but populated only when an inode crosses a block boundary, so a crafted image with few inodes spanning many blocks leaves most slots holding raw heap contents (the underlying allocator does not zero-initialize POD storage). When OpenDir looks up an attacker-influenced blockIndex (derived from the RootNode superblock field), it reads two of these uninitialized slots and passes them as the left/right bounds of a binary search over _nodesPos, which dereferences the midpoint without bounds checking; if the resulting value happens to match the search key, the returned index is used to read a full node struct from _nodes whose fields	2026-06-05	4.2	CVE-2026-48104

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	feed further directory parsing, forming a chained OOB read primitive that is heap-layout-dependent and not reliably triggerable. The SquashFS handler is enabled by default in stock 7z.dll and the issue triggers during Open() with no interaction beyond opening the file; impact is denial of service from wild-pointer dereference and potential heap information disclosure, with no write primitive. Version 26.01 fixes the issue.			
mcmilk--7-Zip	7-Zip is a file archiver with a high compression ratio. Versions 9.21 through 26.00 contain an off-by-one out-of-bounds read vulnerability in the ParseDependencyExpression function of the UEFI firmware image parser(CPP/7zip/Archive/UefiHandler.cpp). The function validates an attacker-controlled opcode byte using > instead of >= against the element count of the 10-entry kExpressionCommands static array, allowing an opcode value of 10 to read one pointer slot (8 bytes on x64) past the end of the array in .rodata. The out-of-bounds value is then dereferenced as a const char * and passed through strlen and memcpy into the archive's Characts property, which may cause either a denial of service (access violation when the adjacent bytes do not form a valid readable pointer) or a minor information disclosure of an adjacent .rdata string literal into archive metadata. The vulnerability is reached automatically during IInArchive::Open() via the call path OpenFv/OpenCapsule â†’ ParseVolume â†’ ParseSections when processing a SECTION_DXE_DEPEX (0x13) or SECTION_PEI_DEPEX (0x1B) section whose first body byte is 0x0A, and the UEFI handler is enabled by default in stock 7z.dll with signature-based detection for both UEFIC and UEFIF formats. The outcome (crash vs. silent leak) is deterministic per build but linker-layout dependent, with no write primitive and no disclosure of heap data, secrets, or ASLR base addresses. Version 26.01 fixes the issue.	2026-06-05	4.3	CVE-2026-48111
Metasoft -- MetaCRM	A security vulnerability has been detected in Metasoft ç¼Žç%¹è½`ä»¶ MetaCRM 6.4.0. The impacted element is an unknown function of the file develop/systparam/softlogo/upload.jsp. Such manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-01	6.3	CVE-2026-10205
Microsoft-- Copilot Chat (Microsoft Edge)	Improper neutralization of special elements in output used by a downstream component ('injection') in Copilot Chat (Microsoft Edge) allows an unauthorized attacker to disclose information over a network.	2026-06-04	6.5	CVE-2026-47644
Microsoft-- Microsoft 365 Copilot	Improper neutralization of special elements used in a command ('command injection') in M365 Copilot allows an unauthorized attacker to disclose information over a network.	2026-06-04	6.5	CVE-2026-42824
Microsoft-- Microsoft Graph	Exposure of sensitive information to an unauthorized actor in Microsoft Graph allows an authorized attacker to disclose information over a network.	2026-06-04	6.5	CVE-2026-47655
milvus-io--milvus	A vulnerability has been found in milvus-io milvus up to 2.6.13. This vulnerability affects unknown code of the file internal/metastore/kv/rootcoord/kv_catalog.go of the component Grantee ID Hash Handler. The manipulation leads to use of weak hash. The attack needs to be performed locally. The attack's complexity is rated as high. It is stated that the exploitability is difficult. The exploit has been disclosed to the public and may be used. The identifier of the patch is	2026-06-04	4.5	CVE-2026-10814

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	3d932f1c3e065351c4440c27abe1e6479752544d. Applying a patch is the recommended action to fix this issue.			
Mimecast--Incydr	In Mimecast Incydr before 2.6.0, arbitrary file access can occur.	2026-06-05	4.5	CVE-2026-50590
mjperpinosa--stumasy	A vulnerability was found in mjperpinosa stumasy. The affected element is an unknown function of the file application/PHP/objects/updates/add_post.php. Performing a manipulation of the argument up_file_to_post results in unrestricted upload. The attack may be initiated remotely. The exploit has been made public and could be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-04	6.3	CVE-2026-10806
mjperpinosa--stumasy	A vulnerability was determined in mjperpinosa stumasy. The impacted element is an unknown function of the file application/PHP/objects/profiles/change_profile_image.php. Executing a manipulation of the argument pr_profile_image can lead to unrestricted upload. The attack may be launched remotely. The exploit has been publicly disclosed and may be utilized. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-04	6.3	CVE-2026-10807
morgan--morgan	Impact: The morgan logging middleware's :remote-user token extracts the Basic auth username from the Authorization request header and writes it to the log stream without neutralizing control characters. An unauthenticated attacker can send a crafted Authorization Basic header containing CR or LF bytes to inject forged log lines, breaking the one-request-per-line structure of access logs and enabling log forgery against downstream log consumers. The built-in combined, common, default, and short formats are affected, as well as any custom format that references :remote-user. Affected versions: morgan 1.2.0 through 1.10.1. Patches: upgrade to morgan 1.11.0, which neutralizes control characters in the :remote-user token output. Workarounds: use a custom format string that does not include :remote-user.	2026-06-03	5.3	CVE-2026-5078
mr_mat--Remove meta boxes per user role	The Remove meta boxes per user role plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.01. This is due to missing or incorrect nonce validation on the 'remove-meta-boxes-per-user-role' page. This makes it possible for unauthenticated attackers to modify or reset the plugin's per-role meta box visibility settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-02	4.3	CVE-2026-8422
myCred--myCred	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in myCred allows Stored XSS. This issue affects myCred: from n/a through 3.0.4.	2026-06-01	6.5	CVE-2026-42676
NamelessMC--Nameless	NamelessMC is website software for Minecraft servers. In versions 2.2.4 and prior, the OAuth callback handling does not validate the state parameter server-side before exchanging the authorization code. This allows an attacker to capture a valid OAuth callback URL for their own	2026-06-02	5.4	CVE-2026-34460

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	account and cause a victim's browser to navigate to it, resulting in the victim's session being authenticated as the attacker-linked account (OAuth login CSRF / session swapping). This is patched in version 2.2.5.			
NamelessMC-- Nameless	NamelessMC is website software for Minecraft servers. A Reflected Cross-Site Scripting (XSS) vulnerability was discovered in version 2.2.4 in the id parameter of the endpoint `/index.php?route=/queries/user/`. The application reflects user-supplied input from the id parameter into the HTML response without proper sanitization or output encoding. An attacker can craft a malicious URL containing JavaScript code. When a victim visits the crafted URL, the injected script executes in the victim's browser within the context of the vulnerable application. This could allow attackers to execute arbitrary JavaScript, potentially leading to session hijacking, phishing attacks, or manipulation of page content. Version 2.2.5 fixes the issue.	2026-06-02	4.3	CVE-2026-32250
NAVTOR-- NavBox	NAVTOR NavBox through version 4.16.1.20 contains hard-coded credentials within its Windows Communication Foundation (SOAP) implementation. If the SOAP functionality is enabled, a local attacker can extract credentials to bypass the intended transfer workflow. Successful authentication against the SOAP interface grants access to privileged WCF methods, enabling an attacker to write or overwrite files within application-defined paths.	2026-06-04	6.3	CVE-2026-21404
nesquena-- Hermes WebUI	Hermes WebUI prior to v0.51.221 contains a path traversal vulnerability that allows attackers to escape the workspace boundary by supplying symlinks that resolve to files or directories outside the designated workspace root. Attackers can exploit the workspace file and listing APIs, which resolve symlink targets without enforcing that the final path remains within the workspace, to read external host files accessible to the server process and disclose sensitive data such as SSH keys, cloud credentials, or application tokens.	2026-06-04	6.5	CVE-2026-11322
nextcloud-- security- advisories	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 32.0.0 to before 32.0.9, and 33.0.0 to before 33.0.3, when a malicious user has access to a file share of a user, they could use this share token to also access the chunking upload directly and see temporary part files during on going uploads. It is recommended that the Nextcloud Server is upgraded to 32.0.9 or 33.0.3. It is recommended that the Nextcloud Enterprise Server is upgraded to 26.0.13.26, 27.1.11.25, 28.0.14.17, 29.0.16.16, 30.0.17.9, 31.0.14.5, 32.0.9 or 33.0.3	2026-06-01	6.3	CVE-2026-45157
nextcloud-- security- advisories	Nextcloud is an open source content collaboration platform. Prior to version 5.2.6, a missing permissions check allowed users to request reading form submissions of other users. This issue has been patched in version 5.2.6.	2026-06-01	6.5	CVE-2026-45267
nextcloud-- security- advisories	Nextcloud is an open source content collaboration platform. Prior to version 2.7.2, a privilege escalation vulnerability exists in the Approval app that allows a user without sharing permissions to force the system to share a file with approvers. This results in an authorization bypass and privilege escalation, allowing unauthorized distribution of restricted files. This issue has been patched in version 2.7.2.	2026-06-01	6.5	CVE-2026-45275

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud--security--advisories	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 32.0.0 to before 32.0.9, and 33.0.0 to before 33.0.3, an authenticated attacker can access attachments of link shares when knowing the share token, circumventing password protection or download restrictions. It is applicable to any file that is shared directly, as the attacker only needs to know a documentId they own, apart of the mentioned share token. For shared folders the attacker has to know or guess a documentId of a file that is included inside the folder, making it much harder to exploit. The attacker can only extract an attachments, but not the file shared file or folder itself. It is recommended that the Nextcloud Server is upgraded to 33.0.3 or 32.0.9. It is recommended that the Nextcloud Enterprise Server is upgraded to 33.0.3, 32.0.9, 31.0.14.5, 30.0.17.9, 29.0.16.16, 28.0.14.17 or 27.1.11.5	2026-06-01	6.5	CVE-2026-45282
nextcloud--security--advisories	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 32.0.0 to before 32.0.2, and 33.0.0 to before 33.0.1, the files_lock app did not properly validate the ownership of files when processing DAV lock and unlock requests. An authenticated user could lock or unlock files belonging to other users by targeting their absolute WebDAV paths. Additionally, lock tokens were disclosed to unauthorized callers in error responses, allowing attackers to remove token-based locks placed by other users' client applications. It is recommended that the Nextcloud Server is upgraded to 32.0.2 or 33.0.1. It is recommended that the Nextcloud Enterprise Server is upgraded to 31.0.14.4 or 32.0.2 or 33.0.1	2026-06-01	6.3	CVE-2026-45283
nextcloud--security--advisories	Nextcloud is an open source content collaboration platform. From versions 32.0.0 to before 32.0.9, and 33.0.0 to before 33.0.3, when a user shares a folder or file with a Nextcloud Team that includes an external member (a person added via email address who does not have a Nextcloud account), the system automatically creates a public link for that external member. This public link is not displayed in the share section of the folder, so the folder owner has no knowledge of its existence. It is sent via email to the external member. It grants the same permissions (read, write, delete, reshare, download) as the Team's access. An attacker who receives or intercepts this link can access, modify, delete, reshare, and download all data in the shared folder without any further authentication. The folder owner cannot see or revoke the link through the normal sharing interface. This issue has been patched in versions 32.0.9 and 33.0.3.	2026-06-01	6.4	CVE-2026-45285
nextcloud--security--advisories	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 31.0.0 to before 31.0.12, and 32.0.0 to before 32.0.3, a missing check of a relation allowed authenticated users with access to any file comment, to read the content of all comments. It is recommended that the Nextcloud Server is upgraded to 31.0.12 or 32.0.3. It is recommended that the Nextcloud Enterprise Server is upgraded to 21.0.9.20, 22.2.10.35, 23.0.12.31, 24.0.12.30, 25.0.13.25, 26.0.13.22, 27.1.11.22, 28.0.14.13, 29.0.16.10, 30.0.17.5, 31.0.12 or 32.0.3	2026-06-01	6.8	CVE-2026-45810
nextcloud--security--advisories	Nextcloud is an open source content collaboration platform. From version 4.3.0 to before version 5.2.7, a removed collaborator retains unauthorized read access to uploaded respondent files for the affected form. The scope is limited to uploaded files for forms where that user previously had results access. This issue has been patched in version 5.2.7.	2026-06-01	5.3	CVE-2026-45543

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 32.0.0 to before 32.0.9, and 33.0.0 to before 33.0.3, an authentication bypass vulnerability allowed attackers with knowledge of a user's password to circumvent two-factor authentication (2FA) protections. When a user initiated login with valid credentials on a 2FA-enabled account, the system created a temporary session token before enforcing the second factor challenge. This token could be extracted and replayed via HTTP Basic Authentication to gain unauthorized access to authenticated endpoints. It is recommended that the Nextcloud Server is upgraded to 33.0.3 or 32.0.9. It is recommended that the Nextcloud Enterprise Server is upgraded to 33.0.3, 32.0.9, 31.0.14.5, 30.0.17.9 or 29.0.16.16	2026-06-01	5.9	CVE-2026-45690
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 32.0.0 to before 32.0.9, and 33.0.0 to before 33.0.3, a pre-2FA session cookie (created after successful password authentication but before TOTP completion) could be reused as a Bearer token to authenticate against DAV endpoints, granting read/write access and bypassing mandatory two-factor authentication. It is recommended that the Nextcloud Server is upgraded to 33.0.3 or 32.0.9. It is recommended that the Nextcloud Enterprise Server is upgraded to 33.0.3, 32.0.9, 31.0.14.5, 30.0.17.9 or 29.0.16.16	2026-06-01	5.9	CVE-2026-45691
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. From version 33.0.0 to before version 33.1.0, after unlocking a locked Android phone the back-button could be used to bypass the Nextcloud Files app PIN. This issue has been patched in version 33.1.0.	2026-06-01	4.6	CVE-2026-45153
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. From versions 17.0.0 to before 17.0.15, 18.0.0 to before 18.1.12, 19.0.0 to before 19.1.16, 20.0.0 to before 20.1.11, and 21.0.0 to before 21.0.4, a user with READ and CREATE permission, but no UPDATE permission for a team folder can rename files in the team folder. This issue has been patched in versions 17.0.15, 18.1.12, 19.1.16, 20.1.11, and 21.0.4.	2026-06-01	4.3	CVE-2026-45264
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 31.0.0 to before 31.0.14, and 32.0.0 to before 32.0.4, if {lang} is used in the template directory config value, non-admin users can in some cases copy arbitrary files (depending on unix permissions) into their own Nextcloud directory via a path traversal. It is recommended that the Nextcloud Server is upgraded to 32.0.4, 31.0.14. It is recommended that the Nextcloud Enterprise Server is upgraded to 32.0.4, 31.0.14, 30.0.17.7, 29.0.17.12, 28.0.14.15	2026-06-01	4.4	CVE-2026-45279
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. From version 1.3.6 to before version 8.4.0, an improper check allowed users that where provided by LDAP to still authenticate towards user OIDC after they where deleted. This issue has been patched in version 8.4.0.	2026-06-01	4.6	CVE-2026-45284
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. From versions 5.5.13 to before 5.5.17, and 6.2.0 to before 6.2.3, an authenticated user can enumerate users on the same Nextcloud instance by using the Calendar app's endpoint for suggesting attendees. The sharing restrictions, applied to other endpoints, were not effective here. This issue has been patched in versions 5.5.17 and 6.2.3.	2026-06-01	4.3	CVE-2026-45286

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. From version 0.8.0 to before version 1.0.4, the view filter criteria is exposed to users with read-only permissions in Nextcloud Tables. This issue has been patched in versions 1.0.4 and 2.0.0.	2026-06-01	4.3	CVE-2026-45544
nextendweb--Smart Slider 3	The Smart Slider 3 plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 3.5.1.36 via the replaceHTMLImage function. This makes it possible for authenticated attackers, with administrator-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	2026-06-06	4.9	CVE-2026-9197
nextlevelbuilder--GoClaw	A flaw has been found in nextlevelbuilder GoClaw up to 3.11.3. The impacted element is the function handleSave of the file internal/http/tts_config.go of the component RoleAdmin Gateway. This manipulation causes improper privilege management. Remote exploitation of the attack is possible. The exploit has been published and may be used. The project tagged the reported issue as bug.	2026-06-01	6.3	CVE-2026-10217
nextlevelbuilder--GoClaw	A vulnerability has been found in nextlevelbuilder GoClaw up to 3.11.3. This affects the function auth of the file internal/http/evolution_handlers.go. Such manipulation leads to improper authorization. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The project tagged the reported issue as bug.	2026-06-01	5.4	CVE-2026-10218
nextlevelbuilder--GoClaw	A security vulnerability has been detected in nextlevelbuilder GoClaw up to 3.11.3. Affected by this issue is the function Import of the file internal/http/tts_config.go of the component TTS Configuration Endpoint. The manipulation leads to server-side request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. The project tagged the reported issue as bug.	2026-06-02	4.7	CVE-2026-10583
nextlevelbuilder--GoClaw	A weakness has been identified in nextlevelbuilder GoClaw up to 3.11.3. The impacted element is the function TeamTasksTool.executeComplete of the file internal/tools/team_tasks_lifecycle.go of the component Team Task Completion Handler. Executing a manipulation can lead to missing authorization. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. The project tagged the reported issue as bug.	2026-06-02	4.3	CVE-2026-10616
NIC--BIRD	CZ.NIC BIRD Internet Routing Daemon through 2.19.0 contains a stack-based buffer overflow in the BGP AS_PATH mask matching implementation in nest/a-path.c. The as_path_match() function uses a fixed-size stack array of 2048 + 1 pm_pos entries, while parse_path() expands AS_PATH segments from a received BGP UPDATE without enforcing a corresponding capacity limit. When RFC 8654 BGP Extended Messages are enabled and a BIRD filter evaluates an AS path mask expression such as "bgp_path ~ [= ... =]", an established BGP peer can send a long AS_PATH containing more than 2048 expanded ASNs. This causes parse_path()/as_path_match() to write beyond the fixed stack buffer, resulting in a crash of the daemon. NOTE: reportedly, the Supplier's position is that a fix is not being prioritized because all network operators should already be rejecting routes with unusually long attributes.	2026-06-02	6.3	CVE-2026-49943

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
NousResearch--hermes-agent	A weakness has been identified in NousResearch hermes-agent up to 2026.4.30. This affects the function <code>_scan_memory_content</code> of the file <code>tools/memory_tool.py</code> . This manipulation causes injection. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-01	6.3	CVE-2026-10223
NousResearch--hermes-agent	A vulnerability has been found in NousResearch hermes-agent up to 0.12.0. This affects the function <code>resolve_session_by_title</code> of the file <code>hermes_state.py</code> of the component <code>resume Endpoint</code> . Such manipulation of the argument <code>Title</code> leads to authorization bypass. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-07	6.3	CVE-2026-11461
NousResearch--hermes-agent	A security flaw has been discovered in NousResearch hermes-agent up to 2026.4.30. Affected by this issue is the function <code>_sanitize_env_lines</code> of the file <code>hermes_cli/config.py</code> . The manipulation results in injection. It is possible to launch the attack remotely. The attack requires a high level of complexity. The exploitation is known to be difficult. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-01	5.6	CVE-2026-10222
NousResearch--hermes-agent	A security vulnerability has been detected in NousResearch hermes-agent up to 2026.4.30. This vulnerability affects the function <code>_handle_webhook_request</code> of the file <code>gateway/platforms/feishu.py</code> of the component <code>Webhook Endpoint</code> . Such manipulation leads to resource consumption. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-01	5.3	CVE-2026-10224
NousResearch--hermes-agent	A security flaw has been discovered in NousResearch hermes-agent up to 2026.4.23. This affects the function <code>_sync_anthropic_entry_from_credentials_file</code> of the file <code>agent/credential_pool.py</code> of the component <code>Credential Pool Synchronization</code> . The manipulation results in improper authentication. The attack must be initiated from a local position. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-02	5.3	CVE-2026-10548
ntbyk--JTL-Connector for WooCommerce	The JTL-Connector for WooCommerce plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 2.4.1. This is due to missing capability checks and nonce verification on the <code>admin_post_settings_save_woo-jtl-connector</code> action (handled by <code>JtlConnectorAdmin::save()</code>) and on the <code>wp_ajax_downloadJTLLogs</code> and <code>wp_ajax_clearJTLLogs</code> AJAX actions (handled by the global <code>downloadJTLLogs()</code> and <code>clearJTLLogs()</code> functions). This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify arbitrary plugin settings, download a ZIP archive of the connector's developer log files, and delete those log files.	2026-06-02	4.3	CVE-2026-9234
OP-TEE--optee_os	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Prior to version 4.11.0, on many of the ECDH shared secret paths, the public key isn't verified to be a point on the correct curve.	2026-06-03	4.7	CVE-2026-45614

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	By passing approximately 30-40 crafted public keys to OP-TEE, the private key can be reconstructed by a normal world attacker. When calling TEE_DeriveKey the public key is provided with full X and Y values, but the (X, Y) point might not satisfy the $Y^2 == X^3 + aX + b \text{ mod } P$ math for the specific curve that is used. When those public keys aren't rejected, the attacker can select public keys such that each DeriveKey call will leak $d \% r$ where d is the private key and r comes from the relationship between the correct curve and the attacker selected curve. With enough leaked data the Chinese remainder theorem can be used to recover the full private key. Version 4.11.0 fixes the issue.			
OP-TEE--optee_os	OP-TEE is a Trusted Execution Environment (TEE) designed as companion to a non-secure Linux kernel running on Arm; Cortex-A cores using the TrustZone technology. Starting in version 4.3.0 and prior to version 4.11.0, a type confusion vulnerability exists in OP-TEE OS when processing an FFA_MEM_SHARE request from the normal world. This only applies when OP-TEE is configured as an SPMC for S-EL0 SPs, that is, with <code>`CFG_CORE_SEL1_SPMC=y`</code> and <code>`CFG_SECURE_PARTITION=y`</code> . Version 4.11.0 fixes the issue.	2026-06-03	4.4	CVE-2026-45702
open-telemetry--go.opentelemetry.io/otel/baggage	OpenTelemetry-Go is the Go implementation of OpenTelemetry. Versions 1.41.0 and 1.43.0 removed raw-length rejection and it causes <code>`Parse`</code> to process arbitrarily large/invalid baggage headers and log errors, enabling DoS via oversized inputs. Versions 1.42.0 and 1.44.0 fix the issue.	2026-06-04	5.3	CVE-2026-41178
open-telemetry--opentelemetry-ebpf-instrumentation	OpenTelemetry eBPF Instrumentation provides eBPF instrumentation based on the OpenTelemetry standard. Prior to version 0.9.0, OBI exports raw Redis error text as the span status message. Because Redis error replies can contain attacker-controlled or sensitive values, this behavior can exfiltrate tokens, PII, or other confidential input into telemetry backends and inject untrusted text into downstream analysis systems. This issue has been patched in version 0.9.0.	2026-06-02	6.5	CVE-2026-45679
open-telemetry--opentelemetry-ebpf-instrumentation	OpenTelemetry eBPF Instrumentation provides eBPF instrumentation based on the OpenTelemetry standard. Prior to version 0.9.0, OBI's replacement ELF parser trusts section offsets, counts, and string offsets from the executable file. A crafted local ELF can make OBI dereference invalid section pointers or slice past string tables, causing the agent to panic while determining the process language. This issue has been patched in version 0.9.0.	2026-06-02	5.5	CVE-2026-45676
open-telemetry--opentelemetry-ebpf-instrumentation	OpenTelemetry eBPF Instrumentation provides eBPF instrumentation based on the OpenTelemetry standard. Prior to version 0.9.0, OBI replays BPF probe hits into histogram observations by looping once per recorded run count. On busy systems, the run-count delta can become very large, causing the metrics exporter to spend excessive CPU time in a tight loop every collection interval. This issue has been patched in version 0.9.0.	2026-06-02	5.9	CVE-2026-45680
open-telemetry--opentelemetry-ebpf-instrumentation	OpenTelemetry eBPF Instrumentation provides eBPF instrumentation based on the OpenTelemetry standard. Prior to version 0.9.0, the per-CPU message-buffer fallback path uses a 256-byte backup buffer but preserves the original payload size, which can be up to 8KB. If a CPU mismatch occurs, OBI can read beyond the fallback buffer and leak adjacent memory into telemetry. This issue has been patched in version 0.9.0.	2026-06-02	5.9	CVE-2026-45681

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
open-telemetry--opentelemetry-ebpf-instrumentation	OpenTelemetry eBPF Instrumentation provides eBPF instrumentation based on the OpenTelemetry standard. Prior to version 0.9.0, the custom CappedConcurrentHashMap introduced for Java TLS state tracking never removes keys from its insertion-order queue when entries are deleted. In long-running instrumented JVMs, repeated connection churn can therefore grow the queue without bound and exhaust heap memory. This issue has been patched in version 0.9.0.	2026-06-02	5.1	CVE-2026-45682
open-telemetry--opentelemetry-ebpf-instrumentation	OpenTelemetry eBPF Instrumentation provides eBPF instrumentation based on the OpenTelemetry standard. From version 0.7.0 to before version 0.9.0, OBI's log enricher mishandles writev buffers by reading only the first iovec entry but using the total iov_iter.count as the copy length. When log injection is enabled, a crafted multi-segment writev call can make OBI read and overwrite memory beyond the first segment. This issue has been patched in version 0.9.0.	2026-06-02	4.9	CVE-2026-45684
OpenSC--OpenSC	A flaw has been found in OpenSC up to 0.26.1. This affects the function test_kpgen_certwrite of the file src/tools/pkcs11-tool.c of the component pkcs11-tool Key Generation Module. This manipulation causes buffer overflow. The attack is possible to be carried out remotely. The complexity of an attack is rather high. It is indicated that the exploitability is difficult. The exploit has been published and may be used. Patch name: 814f745b3b6d100295f65f1935edd33d520d33ab. It is recommended to apply a patch to fix this issue.	2026-06-01	5	CVE-2026-10275
OpenStack--Ironic	OpenStack Ironic before 35.0.2 allows Boot Script Injection of an iPXE script if the attacker can set node.driver_info or node.instance_info.	2026-06-03	5.8	CVE-2026-46447
OpenStack--Ironic	OpenStack Ironic through before 35.0.2 allows file overwrite via directory traversal during deployment with a crafted ISO image.	2026-06-04	5.9	CVE-2026-48681
OpenStack--Ironic	In OpenStack Ironic 32 before 37.0.0, an unauthenticated malicious user could submit a crafted JSON string to some endpoints on the API or JSON-RPC service and effect a service crash.	2026-06-04	5.3	CVE-2026-50589
OpenStack--Ironic	OpenStack Ironic before 35.0.2 allows a malicious authenticated project admin or manager to read local files on the Ironic conductor via a pxe_template.	2026-06-04	4.9	CVE-2026-44917
Orca Energy--Orca heat pump	Missing authentication and clear-text transmission of data from the heat pumps to the control server, combined with the absence of input validation on aggregated data, can lead to stored XSS that enables theft of cookies from the pump's web control interface. Older Orca heat pump devices communicating with the Orca server over an unencrypted and unauthenticated HTTP connection on a non-secure port specifically enable an attacker to impersonate a legitimate device and inject malicious payloads. This enables the insertion of harmful code directly into the Orca user portal, potentially compromising user accounts, exposing sensitive information, and allowing further unauthorized actions within the portal.	2026-06-01	6.3	CVE-2026-25599
OTRS AG--OTRS	An improper neutralization of active SVG content in OTRS or ((OTRS)) Community Edition ticket article rendering allows attackers to inject specially crafted SVG payloads via email content, leading to browser-side resource exhaustion and denial of service when affected tickets are opened by an agent or customer. The issue can be exploited without JavaScript execution and is not mitigated by the configured Content	2026-06-01	6.5	CVE-2026-48208

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Security Policy (CSP). This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.4.X Please note that ((OTRS)) Community Edition 6.x and before are vulnerable. Products based on the ((OTRS)) Community Edition also very likely to be affected			
OTRS AG--OTRS	An uncontrolled allocation of resources without limits or throttling in the e-mail handling in OTRS allows excessive allocation which may lead to the abortion of the webserver.This issue affects OTRS: * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.4.X Please note that ((OTRS)) Community Edition 6.x, OTRS 7.x and products based on the ((OTRS)) Community Edition also very likely to be affected	2026-06-01	5.7	CVE-2026-48187
OTRS AG--OTRS	An improper Input Validation vulnerability in OTRS Customer Backend module allows to access customer information which are restricted to other groups. Please note that the feature has to be anabled and CustomerGroupSupport has to be used to be affected. This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.4.X	2026-06-01	5.7	CVE-2026-48189
PackageKit--PackageKit	A vulnerability has been found in PackageKit up to 1.3.5. Affected is the function g_file_test of the file src/pk-transaction.c of the component API. Such manipulation of the argument frontend-socket leads to improper authorization. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	2026-06-01	4.3	CVE-2026-10294
Paolo--GeoDirectory	Missing Authorization vulnerability in Paolo GeoDirectory allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects GeoDirectory: from n/a through 2.8.157.	2026-06-01	6.5	CVE-2026-42671
passeum--Passeum Ticketing	The Passeum Ticketing plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 1.0. This is due to the `get_shop_url()` method returning the `shop_name` setting value without sanitization when it begins with "http", combined with insufficient validation in the `validate_shop_name()` function which only checks for empty values and string type. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary external scripts by setting the `shop_name` to an attacker-controlled URL (e.g., `https://attacker.com`), which causes the plugin to enqueue external JavaScript and CSS from the attacker-controlled domain via `wp_register_script()` and `wp_register_style()`. The injected scripts execute on every frontend page containing any Passeum Ticketing shortcode, affecting all site visitors. Please note that this does not affect single-site installations as administrators already have the `unfiltered_html` capability.	2026-06-02	4.4	CVE-2026-7421
pattihis--Simple Custom Login Page	The Simple Custom Login Page plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the color settings fields (Page Background, Form Background, Text Color, Link Color) in versions up to and including 1.0.3. This is due to insufficient input sanitization of the color option values (they were registered with register_setting() and stored via the Settings API/update_option() with no sanitize_callback) combined with the values being output into a <style> block on wp-login.php using esc_attr(), which is incorrect for a CSS context (it does not escape ;, {, }, / or *). This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary CSS rules into the login page that are rendered	2026-06-02	4.4	CVE-2026-10100

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	for all unauthenticated visitors, enabling UI-redress and credential-phishing attacks.			
payaddons--Express Payment For Stripe	The Express Payment For Stripe plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'type' attribute of the [stripe-express] shortcode in versions up to, and including, 1.28.0. This is due to insufficient input sanitization and output escaping on the shortcode attribute value, which is concatenated into an HTML attribute in the rendered output of the register_shortcode() function without being passed through esc_attr() or any other escaping function. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-05	6.4	CVE-2026-8893
pcis--Laiser Tag	The Laiser Tag plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.5. This is due to missing or incorrect nonce validation on the addOptionsPageFields function. This makes it possible for unauthenticated attackers to update the plugin's settings, including the API key, tag blacklist, relevance threshold, batch size, and tagging toggles, via a forged request via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-02	4.3	CVE-2026-9722
planetshaker--EmergencyWP Dead Man's switch & legacy deliverance	The EmergencyWP - Dead Man's switch & legacy deliverance plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4.2. This is due to missing or incorrect nonce validation on the form_settings_ui (settings save handler, procedural include scope) function. This makes it possible for unauthenticated attackers to modify plugin settings including the minimum access role (altering WordPress role capabilities via add_cap/remove_cap), the data-erasure-on-uninstall flag, life-check timing values, the mandator email address, the confirmation page ID, and date/time formats via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-02	4.3	CVE-2026-9732
pnggroup--libpng	LIBPNG is a reference library for use in applications that process PNG (Portable Network Graphics) raster image files. In version 1.8.0, three inter-frame chunk discard paths in the push-mode APNG parser clear the chunk-header flag without consuming the chunk body and CRC, allowing attacker-controlled bytes inside an ignored ancillary chunk to be reinterpreted as a fresh chunk header on the next call to `png_process_data`. Commit faf06924688b62d7c1654b5ceddedbde66ffadb4 fixes the issue.	2026-06-04	5.4	CVE-2026-40930
Popup-Builder--Popup Builder	WordPress Popup Builder 3.49 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by breaking out of option tags in the post_title parameter. Attackers can submit crafted POST requests to the post.php endpoint with script payloads in the post_title field that execute when pages or posts display popup selections.	2026-06-04	6.4	CVE-2019-25744
Printers--Printers Print & Ship	Missing Authorization vulnerability in Printers Printers Print & Ship allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Printers Print & Ship: from n/a through 1.17.0.	2026-06-02	6.5	CVE-2025-52766

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
projectworlds--Online Art Gallery Shop Project	A vulnerability was identified in projectworlds Online Art Gallery Shop Project 1.0. The affected element is an unknown function of the file /admin/adminHome.php. The manipulation of the argument social_insta leads to sql injection. The attack may be initiated remotely. The exploit is publicly available and might be used.	2026-06-04	6.3	CVE-2026-10874
projectworlds--Online Art Gallery Shop Project	A security flaw has been discovered in projectworlds Online Art Gallery Shop Project 1.0. The impacted element is an unknown function of the file /admin/adminHome.ph. The manipulation of the argument social_twitter results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-06-04	6.3	CVE-2026-10875
QloApps--QloApps	QloApps through 1.7.0, fixed in commit 64e9722, contains a weak cryptographic algorithm vulnerability that allows attackers to compromise user credentials by exploiting the use of MD5 for password hashing in the Tools::encrypt() function within classes/Tools.php, which concatenates a static cookie key with the supplied password. Attackers can perform offline brute-force attacks against the MD5 hashes, with the risk compounded by auto-generated 8-character passwords assigned during guest-to-customer account conversion in classes/Customer.php, making credential recovery trivial.	2026-06-02	5.9	CVE-2026-25861
qriouslad--Debug Log Manager Conveniently Monitor and Inspect Errors	The Debug Log Manager - Conveniently Monitor and Inspect Errors plugin for WordPress is vulnerable to Improper Output Neutralization for Logs in all versions up to, and including, 2.5.0. This is due to the `log_js_errors()` AJAX handler being registered for unauthenticated users via `wp_ajax_nopriv_log_js_errors` and gated only by a nonce that is publicly disclosed in every front-end page's HTML through `wp_localize_script()` whenever JavaScript error logging is enabled, providing no real authorization barrier. This makes it possible for unauthenticated attackers to inject arbitrary forged entries into the site's WordPress debug log by supplying attacker-controlled values for the `message`, `script`, `lineNo`, `columnNo`, and `pageUrl` fields - enabling spoofing of error and incident records, obscuring malicious activity within fabricated log noise, and misleading administrators who rely on the log for triage. This vulnerability is only exploitable when the plugin's JavaScript error logging feature is enabled, as the requisite nonce is only published into the page HTML under that condition.	2026-06-06	5.3	CVE-2026-9016
Qualcomm, Inc.--Snapdragon	Information Disclosure when resetting device to factory default settings through powerline interface allows unauthorized access to device configuration.	2026-06-01	6.5	CVE-2025-59601
Qualcomm, Inc.--Snapdragon	Memory Corruption when processing IOCTL requests with mismatched API versions due to concurrent modification of user-space buffer.	2026-06-01	6.4	CVE-2025-59610
Qualcomm, Inc.--Snapdragon	Memory corruption in diagnostic services due to absence of input validation	2026-06-01	6.7	CVE-2025-59611
Qualcomm, Inc.--Snapdragon	Memory corruption in windows drivers while sending incorrect trusted application request	2026-06-01	6.7	CVE-2025-59612
Qualcomm, Inc.--Snapdragon	Memory Corruption when output buffer size is smaller than input buffer size during data copying operation.	2026-06-01	6.7	CVE-2025-59613

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Qualcomm, Inc.-- Snapdragon	Memory Corruption when sending random number generator command with insufficient output buffer size.	2026-06-01	6.7	CVE-2025-59614
Qualcomm, Inc.-- Snapdragon	Information Disclosure when processing advertisement frames with malformed MBSSID elements of insufficient length.	2026-06-01	5.5	CVE-2025-59609
quic-go--quic-go	quic-go is an implementation of the QUIC protocol in Go. Prior to version 0.59.1, an attacker can cause excessive memory allocation in quic-go's HTTP/3 client and server implementations by sending a QPACK-encoded HEADERS frame that decodes into a large trailer field section with many unique field names and/or large values. The implementation builds an `http.Header` for the corresponding `http.Request` or `http.Response`, while only enforcing limits on the size of the QPACK-compressed HEADERS frame, not on the decoded field section. This can lead to memory exhaustion. This is very similar to CVE-2025-64702. The difference is that this issue uses HTTP trailers, rather than HTTP headers, as the attack vector. A misbehaving or malicious peer can cause a denial-of-service (DoS) attack against quic-go's HTTP/3 servers or clients by triggering excessive memory allocation, potentially leading to crashes or resource exhaustion. This affects both servers and clients due to symmetric header construction. Version 0.59.1 enforces RFC 9114 decoded field section size limits for trailers as well. It incrementally decodes QPACK entries and checks the field section size after each entry, aborting the stream if an entry causes the limit to be exceeded.	2026-06-04	5.3	CVE-2026-40898
raja3c--Tiled Gallery Carousel Without JetPack	The Tiled Gallery Carousel Without JetPack plugin for WordPress is vulnerable to stored cross-site scripting via the 'data-image-title' parameter in all versions up to, and including, 3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-02	5.4	CVE-2026-5191
Red Hat--Multicluster Engine for Kubernetes	A flaw was found in NetworkManager. This local privilege escalation vulnerability exists in NetworkManager's dhclient backend when processing malformed Manufacturer Usage Description (MUD) URLs. A local user can exploit this flaw to escalate privileges by triggering a script via a crafted MUD URL, provided an administrator has explicitly configured NetworkManager to use dhclient. This issue does not affect default configurations of NetworkManager.	2026-06-04	6.7	CVE-2026-10805
Red Hat--Red Hat Enterprise Linux 10	An out-of-bounds read flaw was found in the X.Org X server and Xwayland in __glXDisp_ChangeDrawableAttributes(). A wrong size validation check can read a client-controlled number of bytes, exceeding the request buffer, leading to information disclosure. A write path also exists but requires byte-swapped clients which is disabled by default.	2026-06-05	5.5	CVE-2026-50262
Red Hat--Red Hat Enterprise Linux 10	A use-after-free flaw was found in the X.Org X server and Xwayland in CreateSaverWindow(). A client can trigger a use-after-free read after changing window attributes and forcing the screen saver, leading to information disclosure.	2026-06-05	5.5	CVE-2026-50263
Red Hat--Red Hat OpenShift	A flaw was found in OpenShift Container Platform. Completed pods with restartPolicy: Never do not count toward ResourceQuota pod limits, and Kubernetes events are not quota-scoped. A non-privileged user who can create pods in a namespace can exploit this to generate a large volume of	2026-06-01	5	CVE-2026-10533

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Container Platform 4	events that accumulate in etcd, causing API server performance degradation across the cluster.			
Red Hat--Red Hat Quay 3	A flaw was found in Clair. The fetcher component makes outbound HTTP requests to attacker-supplied URLs from manifest layer descriptors without IP or scheme filtering. When PSK authentication is not configured (opt-in, not enforced by default), an unauthenticated attacker can submit a manifest with a URI pointing to internal services or cloud metadata endpoints. The SSRF is reflective for non-200 responses, leaking up to 256 bytes of error body content via CheckResponse error messages. Operator-managed Red Hat Quay deployments auto-configure PSK and are not exposed to the unauthenticated attack vector.	2026-06-01	5.8	CVE-2026-10517
remix-run--react-router	React Router is a router for React. In versions 7.5.1 through 7.13.1, when using Framework Mode with pre-rendering enabled, improper neutralization of the HTTP `Location` header value can permit Cross-Site Scripting (XSS) in the statically generated HTML files if the redirect location comes from an untrusted source. This does not impact applications using Declarative Mode (`<BrowserRouter>`) or Data Mode (`createBrowserRouter/<RouterProvider>`). This is patched in version 7.13.2.	2026-06-02	5.4	CVE-2026-33244
Revolution Slider--Slider Revolution	The Slider Revolution plugin for WordPress is vulnerable to Sensitive Information Exposure in versions 7.0.0 - 7.0.14, via the 'slider.get.full' AJAX Action. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive data including raw social media API credentials: the Instagram OAuth token, Flickr API key, YouTube Data API key, and Facebook App ID, stored in any configured slider's settings.	2026-06-01	4.3	CVE-2026-9048
Revolution Slider--Slider Revolution	The Slider Revolution plugin for WordPress in versions 6.0.0-6.7.55 and 7.0.0-7.0.14 is vulnerable to unauthorized modification of data. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with Contributor-level access and above, to deactivate any active plugin installed on the site.	2026-06-01	4.3	CVE-2026-9050
russellr--Tectite Forms	The Tectite Forms plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3. This is due to missing or incorrect nonce validation on the admin_init function. This makes it possible for unauthenticated attackers to modify the plugin's settings, including the tectite_forms_button option, via a forged request via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-02	4.3	CVE-2026-9599
Samsung Open Source--rlottie	Out-of-bounds read vulnerability in Samsung Open Source rlottie allows Overread Buffers. This issue affects rlottie: before 223a2a41ba4f462e4abe767bebbba49a366c9b9fd.	2026-06-04	6.1	CVE-2026-10305
Samsung Open Source--rlottie	Uncontrolled Recursion vulnerability in Samsung Open Source rlottie allows Oversized Serialized Data Payloads. This issue affects rlottie: before e2d19e3b150e0e4a9586fa90b56fd3061cc98945.	2026-06-04	6.1	CVE-2026-47306

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Samsung Open Source--rlottie	Stack-based buffer overflow vulnerability in Samsung Open Source rlottie allows Overflow Buffers. This issue affects rlottie: before ce72b35a7ad0dded03051d3aa0ef75321c3bd035.	2026-06-04	6.1	CVE-2026-47318
Samsung Open Source--rlottie	Memory allocation with excessive size value vulnerability in Samsung Open Source rlottie allows Excessive Allocation. This issue affects rlottie: before 0b4e308fa88c72cbb60cc8a2c1d2c2ad89b101dd.	2026-06-04	6.1	CVE-2026-47319
Samsung Open Source--rlottie	Access of uninitialized pointer, Uncontrolled Recursion vulnerability in Samsung Open Source rlottie allows Pointer Manipulation, Oversized Serialized Data Payloads. This issue affects rlottie: before eae37633fda13ac05b25c6c95aacea4bc33c80a3.	2026-06-04	6.1	CVE-2026-47320
Samsung Open Source--rlottie	Integer overflow or wraparound vulnerability in Samsung Open Source rlottie allows Integer Attacks. This issue affects rlottie: before 21292665023e5074b38254432716866d00f1985f.	2026-06-04	6.1	CVE-2026-49510
Samsung Open Source--rlottie	Out-of-bounds write vulnerability in Samsung Open Source rlottie allows Overflow Buffers. This issue affects rlottie: before dcfde72eae1b0464dc0dd760aec00ada6a148635.	2026-06-04	6.1	CVE-2026-8916
Sekander Badsha--Crew HRM	Missing Authorization vulnerability in Sekander Badsha Crew HRM allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Crew HRM: from n/a through 1.2.2.	2026-06-02	5.4	CVE-2026-27351
Siemens--RUGGEDCOM RST2428P	A vulnerability has been identified in RUGGEDCOM RST2428P (6GK6242-6PA00) (All versions < V4.0). The affected applications stores sensitive information in the browser cache when an authenticated user modify specific configurations. This could allow an authenticated attacker to access sensitive data stored in the browser.	2026-06-02	5.7	CVE-2026-41918
smub--Charitable Donation Plugin for WordPress Fundraising with Recurring Donations & More	The Charitable - Donation Plugin for WordPress - Fundraising with Recurring Donations & More plugin for WordPress is vulnerable to Insecure Direct Object Reference / Authorization Bypass leading to Arbitrary Attachment Deletion in versions up to, and including, 1.8.11.1 via the profile avatar update flow. This is due to the save_avatar() function in Charitable_Profile_Form calling wp_delete_attachment() on an attachment ID read from the user's 'avatar' meta without validating that the attachment is owned by the user, combined with Charitable_Data_Processor::process_picture() returning the raw posted value when no file is uploaded, allowing the 'avatar' user meta to be poisoned with any attacker-chosen attachment ID. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary attachments from the Media Library by performing a two-request chain (first poisoning the stored avatar meta value with a target attachment ID, then triggering deletion via a normal avatar upload).	2026-06-05	4.3	CVE-2026-10038
smub--WPForms Easy Form Builder for WordPress Contact Forms, Payment Forms, Surveys, & More	The WPForms - Easy Form Builder for WordPress - Contact Forms, Payment Forms, Surveys, & More plugin for WordPress is vulnerable to Insufficient Verification of Data Authenticity in versions up to and including 1.10.0.1. This is due to the PayPal Commerce webhook endpoint processing unauthenticated JSON webhook payloads without verifying that the request originated from PayPal using the required HMAC-SHA256 webhook signature, and only checking whether the supplied event_type is whitelisted before dispatching the attacker-controlled resource data to handlers that update payment records. This makes it possible for	2026-06-06	5.3	CVE-2026-7792

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	unauthenticated attackers who know a valid PayPal subscription_id to forge PayPal webhook events and modify subscription payment records, such as reactivating a cancelled or suspended subscription by setting its subscription_status to active.			
Soliloquywp-- Soliloquy Lite	WordPress Soliloquy Lite 2.5.6 contains a persistent cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by inserting script tags in the post title field. Attackers can submit POST requests to the post editing endpoint with script payloads in the post_title parameter, which are stored and executed when users preview the post.	2026-06-04	6.4	CVE-2019-25743
SourceCodester-- Human Resource Management	A vulnerability has been found in SourceCodester Human Resource Management 1.0. Affected by this vulnerability is an unknown functionality of the file /detailview.php of the component Employee View Page. Such manipulation of the argument employeeid leads to improper control of resource identifiers. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	2026-06-02	4.3	CVE-2026-10624
SourceCodester-- Online Boat Reservation System	A security vulnerability has been detected in SourceCodester Online Boat Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the component Administrative Endpoint. The manipulation leads to improper authorization. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used. Multiple endpoints are affected.	2026-06-03	6.3	CVE-2026-10693
SourceCodester-- Pet Grooming Management Software	A flaw has been found in SourceCodester Pet Grooming Management Software 1.0. Affected is an unknown function of the file /admin/. This manipulation causes file and directory information exposure. The attack can be initiated remotely. The exploit has been published and may be used.	2026-06-01	5.3	CVE-2026-10254
SourceCodester-- Pharmacy Sales and Inventory System	A vulnerability has been found in SourceCodester Pharmacy Sales and Inventory System 1.0. Affected by this vulnerability is the function sell_statement of the file application/controllers/ShowForm.php. Such manipulation leads to improper access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2026-06-01	5.3	CVE-2026-10255
SourceCodester-- Pharmacy Sales and Inventory System	A vulnerability was determined in SourceCodester Pharmacy Sales and Inventory System up to 1.0. This issue affects the function create_supplier of the file /Export_csv/export of the component Supplier Creation Interface. This manipulation of the argument Address/Company Name causes csv injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized.	2026-06-01	4.7	CVE-2026-10248
SourceCodester-- Pizzafy Ecommerce System	A vulnerability was detected in SourceCodester Pizzafy Ecommerce System 1.0. Impacted is an unknown function of the file /admin/index.php. Performing a manipulation of the argument page results in file inclusion. The attack is possible to be carried out remotely. The exploit is now public and may be used.	2026-06-02	6.3	CVE-2026-10558
SourceCodester-- Pizzafy Ecommerce System	A flaw has been found in SourceCodester Pizzafy Ecommerce System 1.0. The affected element is an unknown function of the file /index.php. Executing a manipulation of the argument page can lead to file inclusion.	2026-06-02	6.3	CVE-2026-10559

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The attack may be performed from remote. The exploit has been published and may be used.			
SourceCodester--Ship Ferry Ticket Reservation System	A weakness has been identified in SourceCodester Ship Ferry Ticket Reservation System 1.0. This affects an unknown function of the file /admin/. This manipulation of the argument page causes improper authorization. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	2026-06-04	6.3	CVE-2026-10876
SourceCodester--Water Billing Management System	A vulnerability was found in SourceCodester Water Billing Management System 1.0. Impacted is an unknown function of the file /admin/?page=user/manage_user of the component User Management Module. Performing a manipulation of the argument ID results in sql injection. Remote exploitation of the attack is possible. The exploit has been made public and could be used.	2026-06-01	4.7	CVE-2026-10237
spacetime--Ad Inserter Ad Manager & AdSense Ads	The Ad Inserter - Ad Manager & AdSense Ads plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via URL Parameters in iframe Mode in all versions up to, and including, 2.8.15 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. Exploitation requires that iframe mode (AI_OPTION_IFRAME) is enabled on at least one ad block displayed on the targeted page, which is a non-default but supported configuration commonly used for AdSense and JavaScript-based ads.	2026-06-06	6.1	CVE-2026-9280
Spring--Spring Cloud Function	Under infinite recursion in the routing layer, request-handling can cause OOM error. Affected Spring Products and Versions: Spring Cloud Function 3.2.x: versions prior to 3.2.16 Spring Cloud Function 4.1.x: versions prior to 4.1.10 Spring Cloud Function 4.2.x: versions prior to 4.2.6 Spring Cloud Function 4.3.x: versions prior to 4.3.3 Spring Cloud Function 5.0.x: versions prior to 5.0.2 Older, unsupported versions are also affected.	2026-06-01	5.7	CVE-2026-40989
Spring--Spring Cloud Function	OOM error is possible while attempting to add infinite amount of functions to Function Registry. Affected Spring Products and Versions: Spring Cloud Function 3.2.x: versions prior to 3.2.16 Spring Cloud Function 4.1.x: versions prior to 4.1.10 Spring Cloud Function 4.2.x: versions prior to 4.2.6 Spring Cloud Function 4.3.x: versions prior to 4.3.3 Spring Cloud Function 5.0.x: versions prior to 5.0.2 Older, unsupported versions are also affected.	2026-06-01	5.7	CVE-2026-40990
spyrosvl--Simple SEO Slideshow	The Simple SEO Slideshow plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 1.2.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. WordPress KSES does not strip malicious shortcode attribute values on post save, allowing contributor-level users to persist payloads that execute for any visitor, including administrators reviewing the post.	2026-06-05	6.4	CVE-2026-8900
steipete--CodexBar	CodexBar prior to 0.32.0 contains a session cookie leakage vulnerability that allows network attackers to intercept imported browser session cookies by exploiting improper redirect handling for Amp and Ollama provider sessions. Attackers can position themselves on the network path to receive cleartext HTTP requests carrying imported session cookies when	2026-06-01	5.9	CVE-2026-43625

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a provider-controlled redirect target issues a redirect to a cleartext HTTP endpoint within the same provider domain.			
StormShield-- StormShield Network Security	A vulnerability was discovered on Stormshield Network Security * 4.3.0 to 4.3.41, * 4.8.0 to 4.8.15, * 5.0.0 to 5.0.5 It is possible to execute a reflected XSS attack on the login API available on Stormshield SNS appliance by executing a script on the victim's machine. The risks include the theft of cookies or other sensitive data, as well as the modification of page behavior, for example, by redirecting the victim to malicious websites.	2026-06-01	5.3	CVE-2026-8474
strawberry-graphql-- strawberry	Strawberry GraphQL is a library for creating GraphQL APIs. In versions 0.71.0 through 0.315.6, the QueryDepthLimiter extension is vulnerable to an Application-level DOS due to a lack of cycle detection in fragment spreads. When a query contains circular fragment references the determine_depth function enters an infinite recursion, leading to a RecursionError and crashing the validation process. Version 0.315.7 patches the issue.	2026-06-04	5.3	CVE-2026-47706
strawberry-graphql-- strawberry	Strawberry GraphQL is a library for creating GraphQL APIs. In versions 0.172.0 through 0.315.6, the MaxAliasesLimiter extension in Strawberry fails to account for the multiplicative/amplification effect of FragmentSpreadNode. While it correctly counts static aliases within the AST it does not consider how many times a fragments internal aliases are expanded during execution. this allows an attacker to bypass alias limits and force the server to resolve and render a significantly higher number of aliases than allowed, potentially leading to a dos via resource exhaustion. Version 0.315.7 contains a fix for the issue.	2026-06-04	5.3	CVE-2026-47707
StylemixThemes-- MasterStudy LMS Pro	The MasterStudy LMS Pro Plus plugin for WordPress is vulnerable to generic SQL Injection via the 'columns' parameter in all versions up to, and including, 4.8.20 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with instructor-level access or above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-06-04	6.5	CVE-2026-8653
Synology--Hyper Backup	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in Backup.Repository webapi component in Synology Hyper Backup before 4.1.2-4036 allows remote authenticated users with administrator privileges to write specific files containing non-sensitive information via unspecified vectors.	2026-06-03	4.1	CVE-2024-47263
Synology--Hyper Backup	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in Backup Task functionality in Synology Hyper Backup before 4.1.2-4036 allows remote authenticated users to write specific files via unspecified vectors.	2026-06-03	4.3	CVE-2024-47273
Synology-- Synology Note Station Client	A cleartext transmission of sensitive information vulnerability in Synology Note Station Client before 2.2.4-703 allows man-in-the-middle attackers to obtain user credential.	2026-06-03	5.9	CVE-2023-52951
takien--Word Replacer	The Word Replacer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'replacement' parameter in all versions up to, and including, 0.4. This is due to insufficient input sanitization and output	2026-06-02	4.4	CVE-2026-3620

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
themeisle--RSS Aggregator by Feedzy Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator	The RSS Aggregator by Feedzy - Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.1.7. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to create and execute RSS import jobs, purge (force-delete) all posts associated with any import job, clear import error logs, and enumerate taxonomy terms and post meta_key names. The nonce required to reach these sub-handlers is leaked to any user with the edit_posts capability via the feedzyjs localized script injected into the block editor, meaning no privileged nonce theft or separate exploit step is required for Contributor-level users.	2026-06-05	4.3	CVE-2026-8976
theonedev--onedev	A vulnerability has been found in theonedev onedev up to 15.0.5. Affected by this vulnerability is an unknown functionality of the file /projects. The manipulation of the argument project.forkedFromId leads to improper authorization. The attack is possible to be carried out remotely. Upgrading to version 15.0.6 addresses this issue. Upgrading the affected component is recommended.	2026-06-06	6.3	CVE-2026-11438
theonedev--onedev	A vulnerability was found in theonedev onedev up to 15.0.5. Affected by this issue is some unknown functionality of the file /projects/ of the component Parent Project Handler. The manipulation of the argument project.parentId results in improper authorization. The attack may be performed from remote. Upgrading to version 15.0.6 can resolve this issue. It is recommended to upgrade the affected component.	2026-06-06	6.3	CVE-2026-11439
theonedev--onedev	A vulnerability was determined in theonedev onedev up to 15.0.5. This affects an unknown part of the file /repositories/{projectId}/default-branch of the component REST API. This manipulation of the argument project.defaultBranch causes improper authorization. It is possible to initiate the attack remotely. Upgrading to version 15.0.6 is able to mitigate this issue. Upgrading the affected component is advised.	2026-06-06	6.3	CVE-2026-11440
theonedev--onedev	A vulnerability was identified in theonedev onedev up to 15.0.5. This vulnerability affects the function canAccessIssue of the file /issues/ of the component Pull Request Handler. Such manipulation of the argument issue leads to improper authorization. It is possible to launch the attack remotely. Upgrading to version 15.0.6 is able to resolve this issue. It is advisable to upgrade the affected component.	2026-06-06	6.3	CVE-2026-11441
thimpress--LearnPress Backup & Migration Tool	The LearnPress - Backup & Migration Tool plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 4.1.4 via deserialization of untrusted input . This makes it possible for authenticated attackers, with administrator-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary	2026-06-06	6.6	CVE-2026-7566

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	files, retrieve sensitive data, or execute code depending on the POP chain present.			
thimpress-- LearnPress Backup & Migration Tool	The LearnPress - Backup & Migration Tool plugin for WordPress is vulnerable to Arbitrary File Read via Directory Traversal in all versions up to, and including, 4.1.4 via the 'import-user-file' parameter parameter. This makes it possible for authenticated attackers, with administrator-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	2026-06-06	4.9	CVE-2026-7565
thimpress-- LearnPress WordPress LMS Plugin for Create and Sell Online Courses	The LearnPress - WordPress LMS Plugin for Create and Sell Online Courses plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 4.3.6 via the 'return_type' parameter. This makes it possible for unauthenticated attackers to extract sensitive data including the plaintext post_password of password-protected courses and the full post_content, post_author, and post_name of unpublished draft, private, and pending courses via the unrestricted SELECT * fallback query. Exploitation requires supplying both c_status=all (to bypass the publish-only post_status WHERE clause) and return_type=json (to prevent the safe DISTINCT(ID) AS ID field override) in a single unauthenticated request to the /wp-json/lp/v1/courses/archive-course endpoint.	2026-06-06	5.3	CVE-2026-8502
ThimPress--Thim Core	Missing Authorization vulnerability in ThimPress Thim Core allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Thim Core: from n/a through 2.3.3.	2026-06-02	4.3	CVE-2025-53346
thorvg--thorvg	Thor Vector Graphics (ThorVG) is a production-ready vector graphics engine. Prior to version 1.0.5, a null pointer dereference in SvgLoader::run() allows any caller that passes untrusted SVG data to Picture::load() to crash the process with a 6-byte payload. This issue has been patched in version 1.0.5.	2026-06-01	4.3	CVE-2026-45729
Tiobon-- Employee Self- Service System	A vulnerability was found in Tiobon Employee Self-Service System up to 7.2. Affected by this vulnerability is an unknown functionality of the file /Blog/BlogSearch.aspx of the component Login Endpoint. The manipulation of the argument Keyword results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-07	6.3	CVE-2026-11453
Tips and Tricks HQ--WP eMember	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Tips and Tricks HQ WP eMember allows Retrieve Embedded Sensitive Data. This issue affects WP eMember: from n/a through v10.2.2.	2026-06-04	5.3	CVE-2026-49077
tittuvarghese-- CollegeManage mentSystem	A security vulnerability has been detected in tittuvarghese CollegeManagementSystem 3e476335cfbfb9a049e09f474c7ec885f69a9df3/a38852979f7e27ae67b610dce5979500ef8ebe01. The impacted element is an unknown function of the file dashboard_page/forms/upload_student_data.php of the component Student Data Upload Endpoint. Such manipulation of the argument Student-Data-CSV leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. This product takes the approach of rolling releases to provide continuous delivery. Therefore, version details for affected and	2026-06-05	6.3	CVE-2026-11333

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.			
tittuvarghese--CollegeManagementSystem	A flaw has been found in tittuvarghese CollegeManagementSystem 3e476335cfbfb9a049e09f474c7ec885f69a9df3/a38852979f7e27ae67b610dce5979500ef8ebe01. This impacts the function session_start of the file /login-form.php. Executing a manipulation of the argument UserAuthData can lead to session fixation. The attack can be launched remotely. The exploit has been published and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-05	6.3	CVE-2026-11335
tittuvarghese--CollegeManagementSystem	A vulnerability has been found in tittuvarghese CollegeManagementSystem 3e476335cfbfb9a049e09f474c7ec885f69a9df3/a38852979f7e27ae67b610dce5979500ef8ebe01. Affected is an unknown function of the file dashboard_page/admin_page.php of the component Admin Interface. The manipulation of the argument UserAuthData leads to improper authorization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-05	6.3	CVE-2026-11336
tittuvarghese--CollegeManagementSystem	A vulnerability was found in tittuvarghese CollegeManagementSystem 3e476335cfbfb9a049e09f474c7ec885f69a9df3/a38852979f7e27ae67b610dce5979500ef8ebe01. Affected by this vulnerability is an unknown functionality of the file /dashboard_page/forms/fetch.php. The manipulation of the argument department_name results in cross site scripting. The attack may be launched remotely. The exploit has been made public and could be used. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-05	4.3	CVE-2026-11337
Trac d.o.o.--PDBM	The PDBM application relies on a static, hard-coded secret embedded in the PDBM.exe executable. This secret is used by the application's encryption routines, including the function responsible for decrypting credentials stored in the product's configuration file. Because the secret is constant across installations, any attacker with sufficient local privileges can extract it from the binary. Once obtained, the secret allows the attacker to decrypt the stored password and authenticate as the user defined in the configuration file. In the affected version, this user account is configured with administrative privileges, granting full access to PDBM's management interface and its underlying operational functions.	2026-06-01	6.4	CVE-2026-25600
vertex-app--vertex	A vulnerability was identified in vertex-app vertex up to 2026.02.12. This issue affects some unknown processing of the file app/model/LogMod.js of the component Log Viewer Endpoint. Such manipulation of the argument req.query leads to os command injection. The attack can be executed remotely. The exploit is publicly available and might be used. The name of	2026-06-06	6.3	CVE-2026-11408

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the patch is 805d82e7100d49b79b3beb1b9420e8e458987198. It is best practice to apply a patch to resolve this issue.			
warmcat--libwebsockets	A flaw has been found in warmcat libwebsockets up to 4.5.8. This issue affects the function lws_ssh_parse_plaintext of the file plugins/protocol_lws_ssh_base/sshd.c of the component SSH Protocol Handler. Executing a manipulation of the argument msg_len can lead to resource consumption. The attack may be launched remotely. The exploit has been published and may be used. This patch is called 3f9f0c6ecaf0e6f3f219d30632c5d1f2479d7498. A patch should be applied to remediate this issue.	2026-06-02	5.3	CVE-2026-10650
Web-Dorado--Contact Form Maker	Contact Form by WD 1.13.1 contains a cross-site request forgery vulnerability combined with local file inclusion that allows unauthenticated attackers to include arbitrary files by exploiting unsanitized action parameters. Attackers can craft malicious forms targeting the admin-ajax.php endpoint with directory traversal sequences in the GET action parameter to load files via CSRF, bypassing authentication on vulnerable AJAX actions.	2026-06-04	4	CVE-2019-25734
webvitaly--Page-list	The Page-list plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 6.2. This is due to the pagelist_unqprfx_ext_shortcode() function (the [pagelist_ext] / [pagelistext] shortcode) accepting attacker-controlled post_status, post_type, and show_meta_key attributes and passing them directly into get_pages() and get_post_meta() with no capability check verifying that the rendering user is permitted to read the matched objects. When the current post has no child pages, the shortcode re-issues the query with child_of => 0, broadening it to every page on the site matching the supplied status/type. This makes it possible for authenticated attackers, with contributor-level access and above, to disclose the titles, body content/excerpts, and arbitrary post meta of unrelated private and draft pages by inserting the shortcode into a contributor-authored draft and previewing it.	2026-06-06	4.3	CVE-2026-9008
wireapp--wire-ios	wire-ios is an iOS client for the Wire secure messaging application. Prior to version 4.16.0, upon receiving a crafted malicious Proteus external message with an encrypted payload that is shorter than 16 bytes, the Wire iOS client crashes. The crash is triggered automatically after message receival with no user interaction. Since the malicious message persists in the conversation, the app enters a crash loop on relaunch and cannot be reopened until the local state is wiped. This issue has been fixed with version 4.16.0 which introduces the missing length check and is available via the App Store. No known workarounds are available.	2026-06-02	6.5	CVE-2026-35049
wonderwhy-er--DesktopCommanderMCP	A vulnerability was identified in wonderwhy-er DesktopCommanderMCP 0.2.37. This affects the function readFromFileFromUrl of the file src/tools/filesystem.ts of the component read_file. Such manipulation of the argument url leads to server-side request forgery. The attack may be performed from remote. The exploit is publicly available and might be used. The name of the patch is 53699bebbba9950047bca16ac4dc8f0568f596aaa. It is best practice to apply a patch to resolve this issue.	2026-06-02	6.3	CVE-2026-10690

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wonderwhy-er--DesktopCommanderMCP	A security flaw has been discovered in wonderwhy-er DesktopCommanderMCP up to 0.2.38. This impacts an unknown function of the file src/search-manager.ts of the component start_search. Performing a manipulation of the argument SearchResult[] results in inefficient regular expression complexity. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks. Upgrading to version 0.2.39 will fix this issue. The patch is named 4ce845f8749b6a159b57b38dcc3357f7222a8078. It is suggested to upgrade the affected component.	2026-06-02	4.3	CVE-2026-10691
wpdevteam--EmbedPress PDF Embedder, Embed PDF viewer, YouTube Videos, 3D FlipBook, Social feeds & more	The EmbedPress - PDF Embedder, Embed PDF viewer, YouTube Videos, 3D FlipBook, Social feeds & more plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the block 'url' attribute in all versions up to, and including, 4.5.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page	2026-06-06	6.4	CVE-2026-7796
wpdevteam--Essential Addons for Elementor Popular Elementor Templates & Widgets	The Essential Addons for Elementor - Popular Elementor Templates & Widgets plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 6.6.4 via the ajax_load_more function due to insufficient restrictions on which posts can be included. This makes it possible for unauthenticated attackers to extract data from password protected, private, or draft posts that they should not have access to.	2026-06-06	5.3	CVE-2026-7665
zauberzeug--nicegui	NiceGUI is a Python-based UI framework. Prior to version 3.12.0, two FastAPI routes that serve per-component static assets in NiceGUI accept a sub-path parameter that may resolve to a directory rather than a file. Requests that resolve to a directory raise an unhandled RuntimeError inside Starlette's FileResponse, which Uvicorn writes to the server log as a full traceback. Because the routes are reachable without authentication, a remote attacker can amplify log volume and consume disk and log-pipeline capacity on any publicly reachable NiceGUI server. This issue has been patched in version 3.12.0.	2026-06-02	5.3	CVE-2026-45554
zephyrproject-rtos--Zephyr	A potential out-of-bounds write/read exists in the TLS socket connect path of the network sockets subsystem (subsys/net/lib/sockets/sockets_tls.c). When the TLS session cache is enabled, tls_session_store() and tls_session_restore() memcpy the caller-supplied address into a fixed-size buffer using the caller-controlled addrlen value without validating it against the destination size. struct net_sockaddr is an opaque type, so an application can pass an addrlen larger than sizeof(struct net_sockaddr) (for example 128 bytes into a 24-byte stack buffer), causing the memcpy to read and write past the end of the address memory used by the TLS session cache. This out-of-bounds write can lead to a crash and denial of service, and potentially to arbitrary code execution.	2026-06-04	6.3	CVE-2026-5066
zeshanb--Easy Cart	The Easy Cart plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'add_to_cart' shortcode in all versions up to and including 1.8. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes. Specifically, the ectp_add_to_cart() function uses sanitize_text_field() on shortcode attributes like 'itemid', 'product_name', 'product_desc', 'product_qty', and 'price' before inserting	2026-06-02	6.4	CVE-2026-4080

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	them into double-quoted HTML attributes. While <code>sanitize_text_field()</code> strips HTML tags, it does not escape double quote characters, allowing an attacker to break out of the HTML attribute context and inject arbitrary event handlers. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
zeuscart--ZeusCart	ZeusCart 4.0 contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized actions on behalf of victims by crafting malicious requests. Attackers can deactivate customer accounts via the admin interface by tricking users into visiting attacker-controlled pages that submit requests to the <code>regstatus</code> endpoint with <code>action=deny</code> parameters.	2026-06-01	5.3	CVE-2018-25435
zilliztech--deep-searcher	A weakness has been identified in zilliztech deep-searcher up to 0.0.2. This affects the function <code>CollectionRouter.invoke</code> of the file <code>deepsearcher/agent/collection_router.py</code> . This manipulation of the argument <code>kwargs</code> causes improper access controls. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks. The pull request to fix this issue awaits acceptance.	2026-06-07	5.4	CVE-2026-11466
Znuny--Znuny	In Znuny LTS before 6.5.21 and Znuny before 7.3.3, there is reflected XSS in <code>AdminCommunicationLog</code> (aka the communication log administration view).	2026-06-05	6.4	CVE-2026-50592
Znuny--Znuny	In Znuny LTS before 6.5.21 and Znuny before 7.3.3, XSS can occur via stored user preferences.	2026-06-05	5.4	CVE-2026-50591
Zyxel--VMG4005-B50B firmware	A buffer overflow vulnerability in the UPnP <code>AddPortMapping()</code> command in Zyxel VMG4005-B50B firmware versions through 5.13(ABRL.5.4)C0 could allow an adjacent attacker to trigger a temporary denial-of-service (DoS) condition affecting the UPnP function of the affected device.	2026-06-02	6.5	CVE-2026-3870
Zyxel--VMG4005-B50B firmware	A buffer overflow vulnerability in the UPnP <code>DeletePortMapping()</code> command in Zyxel VMG4005-B50B firmware versions through 5.13(ABRL.5.4)C0 could allow an adjacent attacker to trigger a temporary denial-of-service (DoS) condition affecting the UPnP function of the affected device.	2026-06-02	6.5	CVE-2026-3871
100plugins--Open User Map PRO	The Open User Map PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the <code>'oum_location_notification'</code> parameter in versions up to, and including, 1.4.31 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-11	4.7	CVE-2026-2827
2winfactor--Presto Player	The Presto Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the <code>'link_url'</code> parameter of the <code>[presto_player_overlay]</code> shortcode in versions up to, and including, 4.2.0 This is due to insufficient input sanitization and output escaping in the <code>getOverlays()</code> function, which copies the <code>link_url</code> shortcode attribute directly into the overlay configuration without scheme validation, allowing javascript: URIs to survive and be rendered as the href of a clickable anchor element by the <code>presto-dynamic-overlay-ui</code> web component. This makes it possible for authenticated attackers, with contributor-level access and above, to inject	2026-06-12	6.4	CVE-2026-9125

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
360crest--TinyMCE shortcode Addon	The TinyMCE shortcode Addon plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'btnrel' Shortcode Attribute in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-09	6.4	CVE-2026-10024
ABB--Freelance	Authentication bypass by primary weakness vulnerability in ABB Freelance. This issue affects Freelance: through 2013, 2013 SP1, 2016, 2016 SP1, 2019, 2019 SP1, 2019 SP1 FP1, 2024.	2026-06-11	6.6	CVE-2025-7064
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5	CVE-2026-47923
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5	CVE-2026-47924
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5	CVE-2026-47925
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5	CVE-2026-47926
Adobe--Acrobat Reader	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5	CVE-2026-47961
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-34692
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser.	2026-06-09	5.4	CVE-2026-47935

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.			
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47936
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47939
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47941
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47942
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47943
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47944
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47945
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser.	2026-06-09	5.4	CVE-2026-47946

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.			
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-47947
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47948
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47949
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47950
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47951
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47953
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47954
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47956

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	browser when they browse to the page containing the vulnerable field. Scope is changed.			
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47957
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47958
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47962
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47966
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47970
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47972
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47973
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47974

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	browser when they browse to the page containing the vulnerable field. Scope is changed.			
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47975
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47977
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47978
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47980
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47981
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-47982
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-47983
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser.	2026-06-09	5.4	CVE-2026-47985

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.			
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-47986
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-47987
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-47989
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-47990
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-47993
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-48250
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-48251
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser.	2026-06-09	5.4	CVE-2026-48256

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.			
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-48258
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-48264
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-48265
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-48266
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-48268
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-48271
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-06-09	5.4	CVE-2026-48280
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's	2026-06-09	5.4	CVE-2026-48297

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	browser when they browse to the page containing the vulnerable field. Scope is changed.			
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-48299
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-48300
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-48301
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4	CVE-2026-48304
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by an Improper Redirect (Open Redirect) vulnerability that could lead to account takeover. An attacker could construct a malicious URL that redirects a victim to an attacker-controlled site. Exploitation of this issue requires user interaction in that a victim must click on a malicious link.	2026-06-09	4.3	CVE-2026-47991
Adobe--Adobe Experience Manager Forms JEE	Adobe Experience Manager Forms JEE versions LTS SP1, 6.5.24.0 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.9	CVE-2026-34694
Adobe--CAI Content Credentials	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Uncontrolled Resource Consumption vulnerability. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-06-09	6.2	CVE-2026-47902
Adobe--CAI Content Credentials	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Improper Input Validation vulnerability. An attacker could exploit this vulnerability to crash the application, leading to	2026-06-09	6.2	CVE-2026-47903

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	a denial-of-service condition. Exploitation of this issue does not require user interaction.			
Adobe--CAI Content Credentials	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Uncontrolled Resource Consumption vulnerability. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-06-09	6.2	CVE-2026-47904
Adobe--CAI Content Credentials	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Uncontrolled Resource Consumption vulnerability. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-06-09	6.2	CVE-2026-47905
Adobe--CAI Content Credentials	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in an arbitrary file system write. An attacker could leverage this vulnerability to write to unauthorized files or directories outside of intended restrictions. Exploitation of this issue requires user interaction in that a victim must extract a maliciously crafted file.	2026-06-09	5.5	CVE-2026-34657
Adobe--ColdFusion	ColdFusion versions 2023.19, 2025.8 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	4.8	CVE-2026-47933
Adobe--Dreamweaver Desktop	Dreamweaver Desktop versions 21.7 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-06-09	6.3	CVE-2026-47909
Adobe--Dreamweaver Desktop	Dreamweaver Desktop versions 21.7 and earlier are affected by an Incorrect Authorization vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-06-09	6.3	CVE-2026-47910
Adobe--InDesign Desktop	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5	CVE-2026-34703
Adobe--InDesign Desktop	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5	CVE-2026-34704

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Adobe--InDesign Desktop	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5	CVE-2026-34705
AMD--AMD EPYC 7003 Series Processors	Improper input validation for DIMM serial presence detect (SPD) metadata could allow an attacker with physical access, ring0 access on a system with a non-compliant DIMM, or control over the Root of Trust for BIOS update, to potentially overwrite guest memory resulting in loss of guest data integrity.	2026-06-10	5.3	CVE-2024-21944
andrewabarber--Extra Settings for RocketChat	The Extra Settings for RocketChat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'rocketchat' shortcode's 'title' attribute in versions up to, and including, 0.1. This is due to insufficient input sanitization and output escaping in the rxstg_shortcode() function, which concatenates the user-supplied 'title' attribute directly into HTML output. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-09	6.4	CVE-2026-8841
apostrophecms--@apostrophecms/cli	ApostropheCMS is an open-source Node.js content management system. Versions of the @apostrophecms/cli package up to and including 3.6.0 contain a command injection vulnerability in the apos create command. User-supplied input from the password prompt is embedded directly into a shell command without proper sanitization or escaping. This allows execution of arbitrary commands on the host system. As of time of publication, no known patched versions are available.	2026-06-12	6.5	CVE-2026-42853
apostrophecms--sanitize-html	ApostropheCMS is an open-source Node.js content management system, and sanitize-html provides a simple HTML sanitizer with a clear API. Versions of sanitize-html prior to 2.17.5 use 'allowedSchemesAppliedToAttributes' (default: ['href', 'src', 'cite']) to gate the 'naughtyHref()' function that blocks dangerous URI schemes like 'javascript:' and 'vbscript:'. The HTML specification defines 10+ attributes that accept URIs ('action', 'formaction', 'data', 'poster', 'background', 'ping', 'xlink:href', 'dynsrc', 'lowsrc'), but none of these are included in the default gate list. When a developer allows any of these attributes in their configuration, 'javascript:' URIs pass through completely unmodified, enabling XSS. Version 2.17.5 patches the issue.	2026-06-12	5.4	CVE-2026-53606
Aqara--Aqara IAM/SSO Gateway	The Aqara IAM/SSO Gateway (gw-builder.aqara.com) provides an open redirect, which is an instance of "CWE-601: URL Redirection to Untrusted Site," with an estimated CVSS of CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N (6.1 Medium), which can be used to set up a phishing attack.	2026-06-12	6.1	CVE-2026-50089
Aqara--Cloud Developer Portal	The Aqara Cloud Developer Portal (developer.aqara.com) issued a developer token to any email address supplied by the attacker. This is an instance of "CWE-306: Missing Authentication for Critical Function" with an estimated CVSS of CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N (6.5 Medium). When combined with CVE-2026-50083, CVE-2026-50084, and CVE-2026-50085, any otherwise-unauthenticated attacker could execute a full takeover of affected devices.	2026-06-12	6.5	CVE-2026-50082

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aurelienlws--LWS Optimize All-in-One Speed Booster & Cache Tools	The LWS Optimize - All-in-One Speed Booster & Cache Tools plugin for WordPress is vulnerable to Arbitrary File Read in versions up to, and including, 3.3.19. This is due to the <code>combine_current_css()</code> function trusting <code><link rel="stylesheet" href="..."></code> values harvested from page HTML and converting same-site URLs to absolute filesystem paths before reading them with <code>file_get_contents()/Minify\CSS::add()</code> , without enforcing that the resolved path stay within <code>ABSPATH</code> or have a <code>.css</code> extension. This makes it possible for authenticated attackers, with Editor-level access and above, to read arbitrary files.	2026-06-13	4.9	CVE-2026-12089
AWS--s2n-quick	Unbounded memory allocation in the CRYPTO frame reassembler in s2n-quick before 1.8.2 may allow an unauthenticated remote actor to cause a denial of service (degraded availability) by sending crafted QUIC Initial packets. To remediate this issue, users should upgrade to v1.8.2.	2026-06-10	5.3	CVE-2026-10740
axios--axios	Axios is a promise based HTTP client for the browser and Node.js. Prior to 0.32.0 and 1.16.0, axios exposes two read-side prototype-pollution gadgets. When <code>Object.prototype</code> is polluted by an upstream dependency in the same process (e.g. <code>lodash._merge</code> / CVE-2018-16487), axios silently picks up the polluted values. (1) <code>lib/utls.js</code> line 406 builds <code>merge()</code> 's accumulator as <code>result = {}</code> , so <code>result[targetKey]</code> (line 414) walks <code>Object.prototype</code> and the polluted bucket's own keys are copied into the merged headers and ride out on the wire. (2) <code>lib/core/mergeConfig.js</code> line 26 builds the <code>hasOwnProperty</code> descriptor as a plain-object literal. <code>Object.defineProperty</code> reads <code>descriptor.get/descriptor.set</code> via the prototype chain, so a polluted <code>Object.prototype.get</code> or <code>Object.prototype.set</code> makes the call throw <code>TypeError</code> synchronously on every axios request. This vulnerability is fixed in 0.32.0 and 1.16.0.	2026-06-11	4.8	CVE-2026-44490
BeRocket--Advanced AJAX Product Filters	Missing Authorization vulnerability in BeRocket Advanced AJAX Product Filters allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Advanced AJAX Product Filters: from n/a through 1.6.3.3.	2026-06-11	5.4	CVE-2022-45813
boxlite-ai--boxlite	Boxlite is a sandbox service that allows users to create lightweight virtual machines (Boxes) and launch OCI containers within them to run untrusted code. In versions 0.8.2 and prior, Boxlite allows users to configure a timeout for services running inside the virtual machine. When the timeout is triggered, Boxlite sends a signal to kill the process. However, instead of using the uncatchable <code>SIGKILL</code> signal, Boxlite uses the catchable <code>SIGALRM</code> signal. Malicious code running inside the sandbox can exploit this vulnerability to continue running after the timeout is triggered, leading to resource exhaustion within the virtual machine and affecting the availability of the Boxlite service. This issue has been patched via commit 28159fc.	2026-06-10	6.5	CVE-2026-47213
bplugins--Easy Twitter Feeds	Easy Twitter Feeds before 1.2.13 contains a cross-site request forgery vulnerability in the <code>duplicate_post</code> action handler that lacks nonce verification. Attackers can trick an authenticated user into visiting a crafted link that duplicates any post regardless of post type.	2026-06-10	4.3	CVE-2026-53736
brechtvds--Easy Image Collage	The Easy Image Collage plugin for WordPress is vulnerable to Stored Cross-Site Scripting via <code>'grid[properties][borderColor]'</code> and <code>'grid[images][N][attachment_url]'</code> Parameters in all versions up to, and including, 1.13.6 due to insufficient input sanitization and output escaping.	2026-06-10	6.4	CVE-2026-9019

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Because the data is stored via <code>update_post_meta()</code> rather than <code>wp_insert_post()</code> post content, WordPress's <code>unfiltered_html</code> restriction does not apply, meaning Authors cannot be blocked from this attack path by capability controls alone.			
brian-ruf-- OSCAL-GUI	OSCAL-GUI contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to execute arbitrary JavaScript in a victim's browser by injecting malicious input through the project request parameter. Attackers can craft a malicious URL containing unsanitized input that breaks out of the JavaScript string and HTML attribute context in the body onload event handler to execute arbitrary scripts when the link is visited by a victim.	2026-06-09	6.1	CVE-2026-34416
brian-ruf-- OSCAL-GUI	OSCAL-GUI contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to execute arbitrary JavaScript in a victim's browser by injecting malicious content through the project request parameter in <code>oscal-forms.php</code> . The parameter value is URL-decoded and assigned to the <code>project_id</code> variable without sanitization in <code>oscal-functions.php</code> , and when the supplied project ID is not found, the unsanitized value is concatenated into an error message via the <code>Messages()</code> function and reflected into the HTML response body without encoding.	2026-06-09	6.1	CVE-2026-34417
brooks24-- admin-word-count-column	WordPress Plugin admin-word-count-column 2.2 contains a local file read vulnerability that allows unauthenticated attackers to read arbitrary files by exploiting null byte injection in the path parameter. Attackers can send GET requests to <code>download-csv.php</code> with a crafted path parameter containing directory traversal sequences and null bytes to bypass file restrictions and read sensitive files like system configuration.	2026-06-08	6.2	CVE-2022-50953
brthumar1959-- Product Filter Widget for Elementor	The Product Filter Widget for Elementor plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via <code>'args[filterFormArray]'</code> Parameter in all versions up to, and including, 1.0.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. The endpoint is registered via <code>wp_ajax_nopriv_</code> with no nonce verification or capability check, and exploitation is delivered via a CSRF-style form auto-submission to the <code>admin-ajax.php</code> endpoint, requiring the attacker to trick a victim into visiting an attacker-controlled page.	2026-06-09	6.1	CVE-2026-11603
BuddyPress-- BuddyPress	BuddyPress 14.4.0 contains an insecure direct object reference vulnerability in the friends REST API that allows any authenticated attacker to enumerate another user's complete friend list. Attackers can query the friends endpoint with an arbitrary <code>user_id</code> because the <code>get_items_permissions_check</code> method only verifies that the requester is logged in and never checks ownership of the requested list, resulting in disclosure of users' private social connections.	2026-06-09	4.3	CVE-2026-53675
Cap-go--capgo	Cap-go Console < 12.28.2 contains a denial-of-service vulnerability in its account deletion flow that allows an attacker to block authentication and onboarding functions by triggering account deletion while a device identifier is linked to the active session. The platform incorrectly associates	2026-06-12	6.5	CVE-2026-53982

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the deletion state with the device identifier, causing the affected device or browser environment to be redirected to an account-disabled page for approximately 30 days, preventing any account login or registration from that device.			
Cap-go--capgo	Capgo before 12.128.2 fails to delete previously uploaded profile images from backend storage when users replace or remove them. Attackers can access orphaned image files through previously generated URLs, allowing unauthorized retrieval of user-uploaded content.	2026-06-12	4.3	CVE-2026-53867
Chengdu Everbrite Network Technology--BeikeShop	A vulnerability was found in Chengdu Everbrite Network Technology BeikeShop up to 1.6.0.22. Impacted is an unknown function of the file beike/Admin/Routes/admin.php of the component Admin Design Builder Endpoint. Performing a manipulation of the argument settings.value results in sql injection. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The patch is named 2fa9805411088069fcc3b0c15b2f1f33d6e09958. To fix this issue, it is recommended to deploy a patch.	2026-06-08	6.3	CVE-2026-11480
code16--sharp	Sharp is a content management framework built for Laravel as a package. From version 9.0.0 to before version 9.22.3, the create and store endpoints of the Quick Creation Command feature did not enforce any authorization check. An authenticated Sharp user without create permission on a given entity could bypass the authorization layer and either retrieve the creation form or submit new records for that entity, as long as it had a Quick Creation Command handler configured. This issue has been patched in version 9.22.3.	2026-06-10	4.3	CVE-2026-53634
CodeAstro--Human Resource Management System	A weakness has been identified in CodeAstro Human Resource Management System 1.0. This vulnerability affects the function Invoice of the file \application\controllers\Payroll.php of the component Payroll Invoice Module. This manipulation of the argument ID causes sql injection. Remote exploitation of the attack is possible. The exploit has been made available to the public and could be used for attacks.	2026-06-12	6.3	CVE-2026-12131
CodeAstro--Ingredients Stock Management System	A vulnerability was detected in CodeAstro Ingredients Stock Management System 1.0. This impacts an unknown function of the file /Ingredients-Stock/add_stock.php. The manipulation of the argument ID results in sql injection. The attack may be launched remotely. The exploit is now public and may be used.	2026-06-08	6.3	CVE-2026-11495
CodeAstro--Leave Management System	A vulnerability has been found in CodeAstro Leave Management System 1.0. This impacts an unknown function of the file /admin/search_staff_for_deletion.php. The manipulation of the argument Name leads to sql injection. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used.	2026-06-08	6.3	CVE-2026-11506
CodeAstro--Leave Management System	A vulnerability was found in CodeAstro Leave Management System 1.0. Affected is an unknown function of the file /admin/delete_leave_type.php. The manipulation of the argument leave_type results in sql injection. The attack can be executed remotely. The exploit has been made public and could be used.	2026-06-08	6.3	CVE-2026-11507
CodeAstro--Leave	A vulnerability was determined in CodeAstro Leave Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/search_staff_to_assign_pc.php. This manipulation of the argument	2026-06-08	6.3	CVE-2026-11508

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	Name causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.			
CodeAstro--Leave Management System	A vulnerability was identified in CodeAstro Leave Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/search_staff_for_updatation.php. Such manipulation of the argument Name leads to sql injection. The attack may be performed from remote.	2026-06-08	6.3	CVE-2026-11509
CodeAstro--Leave Management System	A security flaw has been discovered in CodeAstro Leave Management System 1.0. This affects an unknown part of the file /admin/add_leave.php. Performing a manipulation of the argument type_of_leave results in sql injection. It is possible to initiate the attack remotely. The exploit has been released to the public and may be used for attacks.	2026-06-08	6.3	CVE-2026-11510
CodeAstro--Payroll System	A security vulnerability has been detected in CodeAstro Payroll System 1.0. The impacted element is an unknown function of the file /home_salary.php. The manipulation of the argument rate/salary_rate leads to sql injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used.	2026-06-08	6.3	CVE-2026-11558
CodeAstro--Payroll System	A vulnerability was detected in CodeAstro Payroll System 1.0. This affects an unknown function of the file /view_account.php. The manipulation of the argument ID results in sql injection. The attack may be performed from remote. The exploit is now public and may be used.	2026-06-08	6.3	CVE-2026-11559
CodeAstro--Student Attendance Management System	A vulnerability has been found in CodeAstro Student Attendance Management System 1.0. This affects an unknown function of the file /attendance-php/Admin/createClass.php. The manipulation of the argument className leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2026-06-08	6.3	CVE-2026-11583
CodeAstro--Student Attendance Management System	A vulnerability was found in CodeAstro Student Attendance Management System 1.0. This impacts an unknown function of the file /attendance-php/Admin/createClass.php?action=edit. The manipulation of the argument ID results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	2026-06-08	6.3	CVE-2026-11584
CodeAstro--Student Attendance Management System	A vulnerability was determined in CodeAstro Student Attendance Management System 1.0. Affected is an unknown function of the file /attendance-php/Admin/createClassArms.php. This manipulation of the argument classId causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2026-06-08	6.3	CVE-2026-11585
CodeAstro--Student Attendance Management System	A vulnerability was detected in CodeAstro Student Attendance Management System 1.0. Impacted is an unknown function of the file /attendance-php/Admin/createStudents.php. Performing a manipulation of the argument admissionNumber results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	2026-06-13	4.7	CVE-2026-12175
codesupplyco--Canvas	The Canvas plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tag' parameter in all versions up to, and including, 2.5.2 due to insufficient input sanitization and output escaping. This makes it	2026-06-13	6.4	CVE-2026-9629

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
ConnectWise--ScreenConnect	In ScreenConnect, versions prior to 26.2, input validation within the Host Pass creation functionality could allow an authenticated user with Host Pass creation privileges the ability to specify a token expiration duration beyond the intended maximum when generating delegated access tokens.	2026-06-10	4.7	CVE-2026-11596
D-Link--DCS-5615	A vulnerability has been found in D-Link DCS-5615 1.01.00. Affected by this vulnerability is an unknown functionality of the file /etc/conf.d/boa/boa.conf of the component Boa Webserver. Such manipulation leads to least privilege violation. The attack can be executed remotely. The exploit has been disclosed to the public and may be used.	2026-06-08	5.3	CVE-2026-11497
D-Link--DIR-823G	A security flaw has been discovered in D-Link DIR-823G 1.0.2B05. The affected element is an unknown function of the file /etc/vsftpd.conf of the component vsftpd. Performing a manipulation results in least privilege violation. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	2026-06-08	4.3	CVE-2026-11492
DALIBO--PostgreSQL Anonymizer	PostgreSQL Anonymizer contains a vulnerability that allows a user to gain superuser privileges by creating a JSON document and placing malicious code inside a particular key-value pair. If a superuser calls the import_database_rules() or import_roles_rules() functions, the malicious code is executed with superuser privileges. The problem is resolved in PostgreSQL Anonymizer 3.1.1 and further versions	2026-06-11	6.4	CVE-2026-11945
Dcat-Admin--Dcat-Admin	A weakness has been identified in Dcat-Admin up to 2.2.3-beta. This impacts the function editorMDUpload of the file /admin/dcat-api/editor-md/upload of the component User Setting Page. This manipulation of the argument editormd-image-file causes unrestricted upload. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks.	2026-06-09	4.7	CVE-2026-11621
Dell--Dell Edge Gateway 3000	Dell Client Platform BIOS contains a Weak Encoding for Password vulnerability. An unauthenticated attacker with physical access could potentially exploit this vulnerability, leading to Elevation of Privileges.	2026-06-09	5.7	CVE-2026-40639
Dell--Dell/Alienware Purchased Apps	Dell/Alienware Purchased Apps, versions prior to 1.1.32.0, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Arbitrary File Write	2026-06-09	6.3	CVE-2026-44275
Dell--iDRAC Tools	Dell iDRAC Tools, versions prior to 11.4.1.0, contains an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information tampering.	2026-06-09	6	CVE-2026-28262
Dell--Inventory Collector Client	Dell Inventory Collector Client, versions prior to 13.8.0, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Arbitrary File Write.	2026-06-09	6.3	CVE-2026-41116

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
designcomputer--mysql-mcp-server	A vulnerability was determined in designcomputer mysql-mcp-server up to 0.2.2. The impacted element is the function read_resource of the file src/mysql_mcp_server/server.py of the component mysql URI Handler. This manipulation of the argument uri_str causes sql injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. Upgrading to version 0.3.0 is sufficient to resolve this issue. Patch name: 080bef9a96d625ce0dfbde573a08b93497871981. Upgrading the affected component is advised.	2026-06-08	6.3	CVE-2026-11529
discourse--discourse	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.4, 2026.3.0-latest to before 2026.3.1, and 2026.4.0-latest to before 2026.4.1, group owners who are not necessarily admins or moderators can view a group's outgoing email/SMTP credentials in plaintext via the group history log (/groups/:name/logs.json). Affected fields: email_password, email_username, smtp_server, smtp_port, smtp_ssl_mode. The most sensitive item is the SMTP password, which an owner could use to send mail as the group from outside Discourse. This impacts sites that have configured per-group SMTP credentials and granted group ownership to users who should not have access to those credentials. This issue has been patched in versions 2026.1.4, 2026.3.1, 2026.4.1, and 2026.5.0-latest.1.	2026-06-12	6.5	CVE-2026-44784
discourse--discourse	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.4, 2026.3.0-latest to before 2026.3.1, and 2026.4.0-latest to before 2026.4.1, a path traversal vulnerability in Discourse backup handling could allow an authenticated administrator on one site in a multisite deployment to access backup files belonging to another site when backups are stored locally. In affected configurations, an admin on Site A could potentially retrieve sensitive backup data from Site B (same host, multisite) by crafting a backup download request with a traversal payload. This issue has been patched in versions 2026.1.4, 2026.3.1, 2026.4.1, and 2026.5.0-latest.1.	2026-06-12	6.8	CVE-2026-45775
discourse--discourse	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.4, 2026.3.0-latest to before 2026.3.1, and 2026.4.0-latest to before 2026.4.1, a flaw in how replies to whisper posts are handled allows authenticated users outside the groups configured in whispers_allowed_groups to post into a topic's staff-only whisper channel. The injected content is visible to whisperers (typically staff) alongside legitimate whispers. Only sites that have whispers enabled are affected. This issue has been patched in versions 2026.1.4, 2026.3.1, 2026.4.1, and 2026.5.0-latest.1.	2026-06-12	5.4	CVE-2026-44783
discourse--discourse	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.4, 2026.3.0-latest to before 2026.3.1, and 2026.4.0-latest to before 2026.4.1, four authorization/disclosure issues in the chat plugin (one also involving discourse-calendar): read-only category users could create chat threads, self-deleted chat messages could be restored by their author after channel access was revoked, moderators reviewing a flagged chat message were shown the channel's current last_message (often unrelated DM content), and calendar event payloads exposed the attached chat channel and its last message to viewers without chat access (including anonymous users). This affects sites with the chat plugin enabled; the calendar issue additionally requires discourse-calendar. This	2026-06-12	5.3	CVE-2026-45085

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	issue has been patched in versions 2026.1.4, 2026.3.1, 2026.4.1, and 2026.5.0-latest.1.			
discourse--discourse	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.4, 2026.3.0-latest to before 2026.3.1, and 2026.4.0-latest to before 2026.4.1, DetailedTagSerializer#tag_group_names returned every tag group a tag belonged to without filtering against the requesting user's visibility. With SiteSetting.tags_listed_by_group enabled, anonymous and unprivileged users hitting TagsController#info (which is exempt from requires_login) could read the names of tag groups restricted to specific user groups or non-visible categories. This issue has been patched in versions 2026.1.4, 2026.3.1, 2026.4.1, and 2026.5.0-latest.1.	2026-06-12	5.3	CVE-2026-47264
discourse--discourse	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.4, 2026.3.0-latest to before 2026.3.1, and 2026.4.0-latest to before 2026.4.1, bot debug endpoints disclose whisper translation audit logs. This issue has been patched in versions 2026.1.4, 2026.3.1, 2026.4.1, and 2026.5.0-latest.1.	2026-06-12	4.3	CVE-2026-44779
discourse--discourse	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.4, 2026.3.0-latest to before 2026.3.1, and 2026.4.0-latest to before 2026.4.1, ReviewableQueuedPostSerializer unconditionally included payload["raw_email"] for posts that arrived via incoming email. Category moderation group members reaching the review queue could therefore read the full inbound email source (headers, sender trace, MUA, body) without being in view_raw_email_allowed_groups - the trust boundary that gates the dedicated raw-email endpoint. This issue has been patched in versions 2026.1.4, 2026.3.1, 2026.4.1, and 2026.5.0-latest.1.	2026-06-12	4.3	CVE-2026-44780
discourse--discourse	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.4, 2026.3.0-latest to before 2026.3.1, and 2026.4.0-latest to before 2026.4.1, GroupPostSerializer declared include_user_long_name? as the predicate for its :name attribute, but AMS looks for include_name?. The misnamed predicate was never called, so object.user.name was always serialized regardless of SiteSetting.enable_names. This issue has been patched in versions 2026.1.4, 2026.3.1, 2026.4.1, and 2026.5.0-latest.1.	2026-06-12	4.3	CVE-2026-44782
discourse--discourse	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.4, 2026.3.0-latest to before 2026.3.1, and 2026.4.0-latest to before 2026.4.1, the AI "explain" helper only checks can_see? on the post being explained, not its reply_to_post, so any authenticated user with access to the AI helper could read the raw contents of a hidden parent post by invoking "Explain" on a reply to it. This issue has been patched in versions 2026.1.4, 2026.3.1, 2026.4.1, and 2026.5.0-latest.1.	2026-06-12	4.3	CVE-2026-44785
discourse--discourse	Discourse is an open-source discussion platform. From versions 2026.1.0-latest to before 2026.1.4, 2026.3.0-latest to before 2026.3.1, and 2026.4.0-latest to before 2026.4.1, the MessageBus.publish call for /web_hook_events/<id> in Jobs::RedeliverWebHookEvents did not pass group_ids, leaving the channel readable by any authenticated user (or anonymous user on instances where login_required is disabled). Webhook IDs are sequential integers and trivially enumerable. This issue has been patched in versions 2026.1.4, 2026.3.1, 2026.4.1, and 2026.5.0-latest.1.	2026-06-12	4.3	CVE-2026-47263

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dolibarr--ERP CRM	A vulnerability was identified in Dolibarr ERP CRM up to 23.0.2. The impacted element is an unknown function of the file <code>htdocs/core/filemanagerdol/connectors/php/config.inc.php</code> of the component Legacy Filemanager. The manipulation leads to improper authorization. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. Upgrading to version 23.0.3 is sufficient to resolve this issue. The identifier of the patch is <code>f1b2dd6481e22cacb561d29ffdc3a50b618479d</code> . Upgrading the affected component is advised.	2026-06-09	6.3	CVE-2026-11619
Ellucian--Banner Self-Service	Ellucian Banner Self-Service before the April T2 release (2025-04-23) contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to execute arbitrary JavaScript in a victim's browser by injecting unsanitized input through the <code>toDateFormat</code> request parameter in the <code>dateConverter</code> endpoint. Attackers can craft a malicious URL targeting the unauthenticated <code>dateConverter</code> endpoint to steal session cookies or perform other malicious actions in the context of the victim's browser session.	2026-06-09	6.1	CVE-2026-32856
Ellucian--Banner Self-Service	Ellucian Banner Self-Service before the April T2 release (2025-04-23) contains a stored cross-site scripting vulnerability in the course search functionality that allows authenticated Banner ERP users to inject malicious payloads into faculty and course fields by exploiting missing HTML encoding during DOM insertion. An attacker with Banner ERP write access can store malicious JavaScript in fields such as <code>faculty displayName</code> , <code>emailAddress</code> , <code>subjectDescription</code> , or <code>courseTitle</code> ; these values are subsequently served unsanitized by the unauthenticated <code>getFacultyMeetingTimes</code> API endpoint, causing arbitrary script execution in the browser of any user who views the affected course's meeting times.	2026-06-09	5.4	CVE-2026-47106
espressif--esp-idf	ESP-IDF is the Espressif Internet of Things (IoT) Development Framework. In versions 5.2.7, 5.3.5, 5.4.4, 5.5.4, and 6.0.1, an out-of-bounds read flaw exists in the DHCP server option parser (<code>parse_options()</code>) in <code>components/lwip/apps/dhcpserver/dhcpserver.c</code> shipped with ESP-IDF's lwIP component. The parser walks the BOOTP/DHCP options field without validating that each option's length byte and declared payload length stay within the received packet buffer. A crafted DHCP request can cause the parser to read past the end of the options buffer into adjacent heap memory. The issue affects the DHCP server used by ESP-IDF's SoftAP and any configuration where the device runs as a DHCP server on a local network. This issue has been patched in versions 5.2.8, 5.3.6, 5.4.5, 5.5.5, and 6.0.2.	2026-06-10	6.5	CVE-2026-45160
espressif--esp-idf	ESP-IDF is the Espressif Internet of Things (IoT) Development Framework. In versions 5.2.6, 5.3.5, 5.4.4, 5.5.3, and 6.0, an out-of-bounds read exists in the BlueDroid AVRCP vendor-command parser (<code>avrc_pars_vendor_cmd()</code>) in <code>components/bt/host/bluedroid/stack/avrc/avrc_pars_tg.c</code> . This issue has been patched in versions 5.2.7, 5.3.6, 5.4.5, 5.5.4, and 6.0.1.	2026-06-10	4.6	CVE-2026-46532
Essential Plugin--WP Logo Showcase Responsive	Authorization bypass through User-Controlled key vulnerability in Essential Plugin WP Logo Showcase Responsive Slider and Carousel allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects WP Logo Showcase Responsive Slider and Carousel: from n/a through 3.6.	2026-06-11	5.3	CVE-2023-40200

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Slider and Carousel				
Eugeniy--russh	Russh is a Rust SSH client & server library. From version 0.37.0 to before version 0.61.0, in the russh client keyboard-interactive authentication path, a malicious SSH server could send a USERAUTH_INFO_REQUEST with an attacker-controlled prompt count, and the client would use that raw count directly in Vec::with_capacity(...) before validating that enough prompt data was actually present in the packet. This issue has been patched in version 0.61.0.	2026-06-10	6.5	CVE-2026-48107
Eugeniy--russh	Russh is a Rust SSH client & server library. From version 0.34.0-beta.1 to before version 0.61.0, the russh server authentication path keeps internal userauth state across SSH_MSG_USERAUTH_REQUEST messages without separating that state when the request principal changes. RFC 4252 allows the user name and service name fields to change between authentication requests. The issue is not that such changes are invalid. The issue is that russh-owned authentication state, such as remaining methods, partial-success state, and in-progress method state, can remain associated with the connection and then influence a later request for a different (user, service). This is an internal library state mismatch. This issue has been patched in version 0.61.0.	2026-06-10	5.3	CVE-2026-46705
Eugeniy--russh	Russh is a Rust SSH client & server library. From version 0.34.0-beta.1 to before version 0.61.0, russh did not enforce the SSH identification-string rules as deliberately as OpenSSH. In particular, the server-side identification reader used the same permissive path as the client, allowing pre-banner lines from clients, and the reader did not enforce a bounded number of pre-banner lines. For a library server built on russh, this could allow a remote peer to hold connection setup resources in the cleartext pre-authentication phase with malformed identification input that should have been rejected early. This issue has been patched in version 0.61.0.	2026-06-10	5.3	CVE-2026-48108
Evoluted--PHP Directory Listing Script	Evoluted PHP Directory Listing Script through 4.0.5 contains a reflected cross-site scripting vulnerability in index.php where the dir parameter value is reflected without HTML encoding inside the HTML title element and inside anchor href attributes in the breadcrumb navigation. Attackers can inject arbitrary JavaScript via crafted dir parameter values by breaking out of the title context or injecting event handlers into breadcrumb anchor attributes to execute malicious scripts in a victim's browser.	2026-06-09	5.4	CVE-2026-25557
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.24.0, Fission builder pods were created with ServiceAccountName: fission-builder and no AutomountServiceAccountToken: false, so the kubelet auto-mounted the service-account token into every container in the pod - including the user-supplied builder image. This issue has been patched in version 1.24.0.	2026-06-10	4.9	CVE-2026-50565
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.25.0, HTTPTriggerSpec.Validate() validated Methods, FunctionReference, Host, IngressConfig, and CorsConfig, but silently skipped RelativeURL and Prefix. Those two fields were validated at the CLI level only (pkg/fission-cli/cmd/httptrigger/create.go:83). The post-CRD-	2026-06-10	4.3	CVE-2026-50569

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	modernization webhook for HTTPTrigger was retired in favor of API-server CEL - and CEL had no rules on those fields either - so an HTTPTrigger created via kubectl apply or a direct Kubernetes REST API call bypassed every URL-level check. This issue has been patched in version 1.25.0.			
Flux159--mcp-server-kubernetes	mcp-server-kubernetes is a Model Context Protocol server for Kubernetes cluster management. Prior to version 3.7.0, the kubectl_generic tool in mcp-server-kubernetes passes user-supplied flags directly to kubectl without any allowlist, enabling a privilege escalation attack within Kubernetes environments. An attacker who already has limited cluster or codebase access, for example, a developer with pod-deployment permissions but not cluster-admin credentials, can plant a single structured JSON line in an application's log output. When an operator with a privileged kubeconfig uses the MCP server to read those logs and their AI agent follows the injected instruction, kubectl_generic is called with --server=https://attacker.example.com and --insecure-skip-tls-verify=true. kubectl sends all API requests, including the Authorization: Bearer <token> header from the operator's kubeconfig to the attacker's endpoint. The captured token can then be replayed directly against the real Kubernetes API server, granting the attacker the full RBAC permissions of the operator's service account. This issue has been patched in version 3.7.0.	2026-06-11	6.1	CVE-2026-47250
fooplugins--Photo Gallery by FooGallery : Responsive Image Gallery, Masonry Gallery & Carousel	The FooGallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'custom_attribute_key' shortcode parameter in versions up to, and including, 3.1.31 This is due to an incomplete JavaScript event handler blacklist in the foogallery_sanitize_javascript() function, which blocks only a subset of HTML event attributes (onmouseover, onmouseout, onpointerenter, onclick, onload, onchange, onerror) while permitting others such as 'onmouseenter', combined with the failure to escape the attribute key when building the gallery container HTML in foogallery_build_container_attributes_safe(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-13	6.4	CVE-2026-9134
Fortinet--FortiOS	An Internal Asset Exposed to Unsafe Debug Access Level or State vulnerability [CWE-1244] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.2, FortiOS 7.4.0 through 7.4.7, FortiOS 7.2.0 through 7.2.10, FortiOS 7.0.0 through 7.0.16, FortiOS 6.4 all versions, FortiProxy 7.6.0 through 7.6.3, FortiProxy 7.4.0 through 7.4.10, FortiProxy 7.2.0 through 7.2.14, FortiProxy 7.0 all versions may allow an authenticated admin to execute lua scripts via crafted CLI commands.	2026-06-09	6	CVE-2025-67862
Fortinet--FortiPortal	A improper access control vulnerability in Fortinet FortiPortal 7.4.0 through 7.4.7, FortiPortal 7.2.0 through 7.2.8, FortiPortal 7.0 all versions may allow attacker to improper access control via <insert attack vector here>	2026-06-09	6.2	CVE-2026-49938
frankverbeke--OpenClinic GA	OpenClinic GA 5.351.19 contains a reflected cross-site scripting vulnerability in the DICOM image upload handler that allows attackers to execute arbitrary JavaScript in a victim's browser by embedding malicious payloads in DICOM file metadata fields. Attackers can craft a DICOM file with JavaScript payloads in metadata fields such as Study Description, which are reflected without sanitization in popup.jsp and	2026-06-09	6.1	CVE-2026-25860

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	archiving/uploadfiles_jsp.java when processed through the Upload DICOM images feature.			
Gen Digital-- Avast Antivirus	Uncontrolled recursion vulnerability in Avast Antivirus when scanning a malformed Windows PE file may allow Denial-of-Service of the antivirus process. This issue affects Avast Antivirus, AVG Antivirus, Norton Antivirus, Avast One, and Avast Business Antivirus on Windows, macOS, and Linux for virus definition builds before VPS 25031700. The affected scanning logic is delivered through a shared Gen Digital virus definition update stream. The same stream feeds the consumer antivirus products listed in this advisory and other Gen Digital products that embed the same engine. Mitigation flows through this update channel; installations at or above the listed build are not vulnerable regardless of which product consumes the stream.	2026-06-12	5.5	CVE-2025-7005
Gen Digital-- Avast Antivirus	Use of stack memory after free vulnerability in Avast Antivirus when scanning a malformed Windows PE file may allow Denial-of-Service of the antivirus process. This issue affects Avast Antivirus, AVG Antivirus, Norton Antivirus, Avast One, and Avast Business Antivirus on Windows, macOS, and Linux for virus definition builds before VPS 25022500. The affected scanning logic is delivered through a shared Gen Digital virus definition update stream. The same stream feeds the consumer antivirus products listed in this advisory and other Gen Digital products that embed the same engine. Mitigation flows through this update channel; installations at or above the listed build are not vulnerable regardless of which product consumes the stream.	2026-06-12	5.5	CVE-2025-7006
Gen Digital-- Avast Antivirus	Stack overflow vulnerability due to uncontrolled recursion in Avast Antivirus when scanning a malformed PDF file may allow Denial-of-Service of the antivirus process. This issue affects Avast Antivirus, AVG Antivirus, Norton Antivirus, Avast One, and Avast Business Antivirus on Windows, macOS, and Linux for virus definition builds before VPS 25021208. The affected scanning logic is delivered through a shared Gen Digital virus definition update stream. The same stream feeds the consumer antivirus products listed in this advisory and other Gen Digital products that embed the same engine. Mitigation flows through this update channel; installations at or above the listed build are not vulnerable regardless of which product consumes the stream.	2026-06-12	5.5	CVE-2025-7010
Gen Digital-- Avast Antivirus	Stack overflow vulnerability in Avast Antivirus when scanning a malformed Office Open XML file may allow Denial-of-Service of the antivirus process. This issue affects Avast Antivirus, AVG Antivirus, Norton Antivirus, Avast One, and Avast Business Antivirus on Windows, macOS, and Linux for virus definition builds before VPS 25020100. The affected scanning logic is delivered through a shared Gen Digital virus definition update stream. The same stream feeds the consumer antivirus products listed in this advisory and other Gen Digital products that embed the same engine. Mitigation flows through this update channel; installations at or above the listed build are not vulnerable regardless of which product consumes the stream.	2026-06-12	5.5	CVE-2025-7019
Gen Digital-- Avira Antivirus	Null pointer dereference vulnerability in Avira Antivirus engine when scanning a malformed Windows PE file may allow Denial-of-Service of the antivirus engine process. This issue affects Avira Antivirus on Windows, macOS, and Linux for engine builds before 8.3.70.64.	2026-06-12	5.5	CVE-2025-7018

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Genspark--AI Workspace App	A vulnerability has been found in Genspark AI Workspace App 2.8.4 on Android. This vulnerability affects unknown code of the component ai.mainfunc.genspark. The manipulation leads to improper authorization in handler for custom url scheme. The attack can only be performed from a local environment. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-14	5.3	CVE-2026-12190
Ghidra--Ghidra	Ghidra before 12.1.1 contains an uncontrolled memory allocation vulnerability in the Mach-O binary parser that allows attackers to cause denial of service. An attacker can supply a crafted Mach-O binary with an arbitrarily large ncmds load command count value, forcing the parser to allocate excessive heap memory without validating file size, crashing the Ghidra JVM.	2026-06-10	5.5	CVE-2026-52759
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.10 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2 that under certain conditions could have allowed an authenticated user to cause denial of service due to uncontrolled resource consumption when processing a specially crafted file upload.	2026-06-11	6.5	CVE-2026-1500
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.10 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2 that under certain conditions could have allowed an authenticated user with developer-role permissions to modify hidden merge requests due to incorrect authorization enforcements.	2026-06-11	5.4	CVE-2026-6269
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 18.10 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2 that under certain conditions could have allowed an authenticated user to read arbitrary files from the Gitaly server and access internal network resources during repository import, due to insufficient validation of secondary URLs.	2026-06-11	5.3	CVE-2026-9204
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.0 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2 that could have allowed an authenticated user to cause denial of service on the CI/CD Catalog page due to improper sanitization.	2026-06-11	4.3	CVE-2026-10733
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 13.9 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2 that under certain conditions could have allowed an authenticated user with Security Manager-role permissions to manage project security configuration even when the relevant feature was in a disabled state, due to incorrect authorization enforcement.	2026-06-11	4.3	CVE-2026-6277
GL.iNet--A1300	A flaw has been found in GL.iNet A1300, AX1800, AXT1800, MT2500, MT3000, MT6000, X3000 and XE3000 4.8.x. This affects an unknown function of the component glnassys. Executing a manipulation can lead to use of hard-coded cryptographic key . The attack may be launched remotely. The attack requires a high level of complexity. The exploitability is reported as difficult. Upgrading to version 4.9.0 mitigates this issue. Upgrading the affected component is advised.	2026-06-08	5	CVE-2026-11505
Grit42--Grit	A vulnerability was detected in Grit42 Grit up to 0.11.0. Affected by this issue is some unknown functionality of the file modules/core/backend/app/controllers/concerns/grit/core/grit_entity_controller.rb of the component GritEntityController. Performing a	2026-06-14	6.3	CVE-2026-12188

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	manipulation results in sql injection. The attack may be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.			
guzzle--guzzle-services	Guzzle Services provides an implementation of the Guzzle Command library that uses Guzzle service descriptions to describe web services, serialize requests, and parse responses into easy to use model structures. Versions prior to 1.5.4 do not safely serialize scalar XML element values containing the CDATA terminator `]]>`. The XML request serializer writes values containing `<`, `>`, or `&` with `XMLWriter::writeCdata(\$value)`. If attacker-controlled input contains `]]>`, the CDATA section closes early and the remainder is interpreted as XML markup. This is an outgoing request-body integrity issue, not a response parsing issue. The attacker does not need to control the service description or schema. Users are affected when all of the following are true: the application uses `guzzlehttp/guzzle-services` to serialize outgoing requests; a request parameter or `additionalParameters` schema uses `location: xml`; the value is serialized as XML element text, not an XML attribute; the value can contain attacker-controlled, user-controlled, tenant-controlled, or otherwise untrusted input; the value is not constrained by a safe `enum`, `pattern`, or custom filter that excludes `]]>`; and the downstream service parses the generated XML structurally and may act on unexpected, duplicated, or injected elements. Applications that serialize untrusted input into `location: xml` request parameters can emit XML containing attacker-controlled elements outside the intended text node. Depending on the receiving service, this can alter operation semantics, smuggle privileged fields, bypass modeled parameter boundaries, or create conflicting duplicated elements. Fixed service descriptions are sufficient if they contain an XML element parameter populated from attacker-controlled input. Users are not directly affected if they only use Guzzle Services to deserialize HTTP response bodies. Response XML parsing uses the response XML location visitor and does not invoke the vulnerable request XML serializer. Response bodies matter only in a second-order flow, such as parsing attacker-controlled response XML, storing or forwarding a parsed string value, and later using it as a `location: xml` request parameter. The issue is patched in `1.5.3` and later by safely splitting embedded CDATA terminators before serialization. The fix preserves the original scalar value as XML text and prevents injected nodes. As a workaround, constrain attacker-controlled XML element values with a strict `enum`, `pattern`, or custom filter that excludes `]]>`, or avoid serializing untrusted data into `location: xml` element text until patched. Where appropriate for the service schema, XML attributes are not affected because they are written with XMLWriter attribute APIs rather than CDATA sections. To determine whether action is needed, search service descriptions for request parameters using `location: xml`, including operation `parameters` and `additionalParameters`. Response-only `models` are not directly affected unless parsed values are reused for request serialization. For object and array parameters, review nested scalar properties because leaf element values can still be affected.	2026-06-11	5.8	CVE-2026-53723
guzzle--psr7	guzzlehttp/psr7 is a PSR-7 HTTP message library implementation in PHP. Versions prior to 2.10.2 contain improper Host header validation when parsing raw HTTP request messages and when deriving a server request URI from server variables. An attacker can provide a malformed Host	2026-06-11	5.3	CVE-2026-48998

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	header containing URI authority delimiters, such as `trusted.example@evil.example`. When the Host value is used to construct a URI, the malformed value can be reinterpreted as URI userinfo and host. This can cause the PSR-7 request URI host to differ from the original Host header value. Applications are affected if they parse attacker-controlled raw HTTP requests with `GuzzleHttp\Psr7\Message::parseRequest()` or the legacy 1.x `GuzzleHttp\Psr7\parse_request()` function, or if they build server requests from attacker-controlled server variables, then rely on the resulting URI host for routing, allow-list checks, or forwarding decisions. In affected forwarding or gateway scenarios, this may cause requests or credentials to be sent to an unintended host. The issue is patched in `2.10.2`. `1.x` is end-of-life and will not receive a patch. Some workarounds are available. Validate the `Host` header as `uri-host [ ":" port ]` before calling `Message::parseRequest()` or legacy `parse_request()` on untrusted HTTP request data, or before deriving routing and forwarding decisions from a parsed request URI. Reject Host values containing userinfo, path, query, or fragment delimiters.			
guzzle--psr7	guzzlehttp/psr7 is a PSR-7 HTTP message library implementation in PHP. Versions prior to 2.10.2 did not reject ASCII control characters, whitespace, or DEL in first-party URI host components. A vulnerable flow is: First, an application accepts a user-controlled URL. Second, the URL is used to construct a PSR-7 `Uri` or `Request`. Third, the host component contains CRLF or another header-unsafe character. Fourth, the host is copied into the PSR-7 `Host` header when no explicit `Host` header is provided. Finally, the request is serialized or sent by an HTTP client that does not independently reject the malformed host. In that flow, an attacker can cause the serialized request to contain additional attacker-controlled header lines. For example, a host containing `""r\nX-Injected: yes""` can cause the generated `Host` header to span multiple HTTP header lines. Applications are affected when they use user-controlled URLs for outbound HTTP requests, URL forwarding, proxying, crawling, webhook delivery, or similar request-dispatch flows. In deployments involving HTTP/1.1 connection reuse, proxies, gateways, or load balancers, this malformed request may also contribute to request smuggling or cache poisoning, depending on how downstream components parse the request. The issue is patched in `2.10.2` and later. `1.x` is end-of-life and will not receive a patch. As a workaround, validate and reject all untrusted URI strings before constructing PSR-7 `Uri` or `Request` instances. Reject input containing ASCII control characters, whitespace, or DEL, including CRLF, tab, space, NUL, or DEL characters. Applications that forward requests should also ensure the final HTTP client or serializer rejects invalid URI and header data before writing requests to the network.	2026-06-11	5.3	CVE-2026-49214
halfgaar--FlashMQ	FlashMQ is a MQTT broker/server, designed for multi-CPU environments. Prior to version 1.26.2, authorized clients have the ability to exceed the permitted over-commit of their write buffer and triggering an internal safe-guard exception. This exception was in a path that was not catchable, and therefore causes a server abort. This issue has been patched in version 1.26.2.	2026-06-09	6.5	CVE-2026-46411
HashThemes--Hash Elements	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in HashThemes Hash Elements allows Retrieve	2026-06-12	4.3	CVE-2026-24618

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Embedded Sensitive Data. This issue affects Hash Elements: from n/a through 1.5.4.			
Hedef Media Promotion Interactive Media Marketing Inc.--Related Marketing Cloud (RMC)	Authentication bypass by spoofing vulnerability in Hedef Media Promotion Interactive Media Marketing Inc. Related Marketing Cloud (RMC) allows Brute Force. This issue affects Related Marketing Cloud (RMC): through 12052026.	2026-06-12	6.5	CVE-2026-5792
helpfulcrowd--Helpfulcrowd Product Reviews	The Helpfulcrowd Product Reviews plugin for WordPress is vulnerable to Authorization Bypass via PHP Type Juggling in versions up to, and including, 1.2.9. This is due to the `helpfulcrowd_validate_token()` function using a loose comparison operator (`!=`) instead of a strict comparison (`!==`) when validating the `token` parameter, while the corresponding REST route `/wp-json/helpfulcrowd/v1/update-settings` is registered with a `permission_callback` of `__return_true`, making it reachable by unauthenticated users; submitting a JSON boolean `true` as the `token` value causes PHP's loose comparison to evaluate as equal to the non-empty base64-encoded secret string, bypassing the check entirely. This makes it possible for unauthenticated attackers to invoke `helpfulcrowd_settings_endpoint()` and write arbitrary attacker-controlled key-value pairs directly into the `helpfulcrowd_options` WordPress database option via `update_option()` without any sanitization or allowlist filtering, enabling full unauthenticated modification of the plugin's stored configuration.	2026-06-09	5.3	CVE-2026-8499
helpstring--Global Body Mass Index Calculator	The Global Body Mass Index Calculator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'gbmicalc' shortcode in versions up to, and including, 1.2. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes in the GBMI_Calc_Widget::widget() function. Shortcode attributes are extracted directly into local variables via @extract(\$args) and then echoed unescaped into an HTML style attribute (height/width) and HTML body context (title), allowing attribute-breakout payloads. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-09	6.4	CVE-2026-8883
Hepta Platforms--Heptabase	Heptabase developed by Hepta Platforms has a Exposed Dangerous Method or Function vulnerability, allowing unauthenticated remote attackers to leverage social engineering techniques to trick a victim into opening or loading a malicious webpage within the Heptabase application, thereby gaining unauthorized access to camera and microphone permissions.	2026-06-12	6.5	CVE-2026-12060
hs-web--hsweb-framework	A vulnerability has been found in hs-web hsweb-framework up to 5.0.1. The affected element is the function denied of the file hsweb-system/hsweb-system-file/src/main/java/org/hswebframework/web/file/FileUploadProperties.java of the component File Upload. The manipulation of the argument filename leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of the patch is	2026-06-08	6.3	CVE-2026-11470

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	8009845b577d8a2c4bbf4fdd8e8913799a714be6. It is suggested to install a patch to address this issue.			
hs-web--hsweb-framework	A vulnerability was detected in hs-web hsweb-framework up to 5.0.1. This affects the function OAuth2Client of the file hsweb-authorization/hsweb-authorization-oauth2/src/main/java/org/hswebframework/web/oauth2/server/OAuth2Client.java of the component OAuth2 Client. The manipulation results in open redirect. The attack can be executed remotely. The exploit is now public and may be used. The patch is identified as c2882679a9125cea52678151af5ae213cbd52579. Applying a patch is advised to resolve this issue.	2026-06-08	4.3	CVE-2026-11477
Huawei--HarmonyOS	Permission management vulnerability in the network management module. Impact: Successful exploitation of this vulnerability may affect service integrity.	2026-06-09	6.3	CVE-2026-41975
Huawei--HarmonyOS	Permission control vulnerability in the audio framework. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-06-09	6.6	CVE-2026-41976
Huawei--HarmonyOS	Race condition vulnerability in the IPC module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	6.4	CVE-2026-41982
Huawei--HarmonyOS	Path traversal vulnerability in the SMS app. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	5.4	CVE-2026-41972
Huawei--HarmonyOS	Permission control vulnerability in calls. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	5.9	CVE-2026-41973
Huawei--HarmonyOS	DoS vulnerability in the log service. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	5	CVE-2026-41977
Huawei--HarmonyOS	Permission control vulnerability in the print module. Impact: Successful exploitation of this vulnerability may affect integrity and confidentiality.	2026-06-09	5.5	CVE-2026-41979
Huawei--HarmonyOS	Permission control vulnerability in the file preview module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-06-09	5.5	CVE-2026-41980
Huawei--HarmonyOS	Out-of-bounds write vulnerability in the IPC module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	5.3	CVE-2026-41981
Huawei--HarmonyOS	UAF vulnerability in the package management module. Impact: Successful exploitation of this vulnerability may affect service integrity.	2026-06-09	5.2	CVE-2026-41984
Huawei--HarmonyOS	UAF vulnerability in the package management module. Impact: Successful exploitation of this vulnerability may affect service integrity.	2026-06-09	5.1	CVE-2026-41985
Huawei--HarmonyOS	Permission control vulnerability in the clone module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-06-09	4.4	CVE-2026-41978
Huawei--HarmonyOS	DoS vulnerability in the browser kernel. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	4.3	CVE-2026-41983
hyperledger--fabric-chaincode-java	fabric-chaincode-java is a Java based implementation of Hyperledger Fabric chaincode shim APIs. From version 2.3.1 to before version 2.5.10, when chaincode is deployed in chaincode-as-a-service mode with TLS	2026-06-08	5.5	CVE-2026-45581

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	enabled, the chaincode server INFO level logging includes the TLS private key password in plaintext. An attacker with access to the chaincode server logs could recover the TLS private key password. If the attacker can also obtain the TLS private key, they could impersonate the chaincode server. This issue has been patched in version 2.5.10.			
IBM--DevOps Plan	IBM DevOps Plan 3.0.0 through 3.0.6 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking	2026-06-11	6.5	CVE-2026-4096
IBM--Langflow Desktop	IBM Langflow Desktop 1.0.0 through 1.9.2 IBM Langflow is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	2026-06-11	5.4	CVE-2026-3341
IBM--Security QRadar EDR	IBM Security QRadar EDR 3.12 through 3.12.24 stores user credentials in plain text which can be read by a local privileged user.	2026-06-11	4.1	CVE-2024-45636
IEI Integration Corp--iRM-TSi410X	The iRM-IEI Remote Management developed by IEI Integration Corp has a Missing Authentication vulnerability, allowing unauthenticated remote attackers to exploit a specific functionality to obtain partial system configuration information.	2026-06-12	5.3	CVE-2026-11848
IEI Integration Corp--iVEC TANK-XM811	The iVEC-IEI Virtualization Edge Computer developed by IEI Integration Corp has a Arbitrary File Read vulnerability, allowing privileged remote attackers to access files outside the intended directory scope.	2026-06-12	4.9	CVE-2026-11844
IEI Integration Corp--iVEC TANK-XM811	The iVEC-IEI Virtualization Edge Computer developed by IEI Integration Corp has a Path Traversal vulnerability, allowing authenticated remote attackers to exploit this vulnerability to create directories in unintended system paths.	2026-06-12	4.3	CVE-2026-11847
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 7.1.2-23 and 6.9.13-48, a crafted MSL image can trigger a heap-use-after-free. Versions 7.1.2-23 and 6.9.13-48 fix the issue.	2026-06-10	6.2	CVE-2026-46523
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to version 7.1.2-23, due to a missing depth check a stack overflow can occur in the fx operation by passing a crafted argument. This issue has been patched in version 7.1.2-23.	2026-06-10	6.2	CVE-2026-46557
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to version 7.1.2-25, a crafted multi-frame can result in a heap buffer over-write when encoding it with the SF3 encoder. This issue has been patched in version 7.1.2-25.	2026-06-10	6.2	CVE-2026-53465
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-47 and 7.1.2-22, when writing an IPTC output file a malicious input file could cause an out of bounds read of a single byte. This issue has been patched in versions 6.9.13-47 and 7.1.2-22.	2026-06-10	5.1	CVE-2026-42326

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-47 and 7.1.2-22, due to a missing check in the PSD decoder it would be possible to bypass the list-length resource policy when decoding a PSD image. Other security limits would still apply. This issue has been patched in versions 6.9.13-47 and 7.1.2-22.	2026-06-10	5.3	CVE-2026-45031
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-47 and 7.1.2-22, an off by one in the meta encoder could result in an out of bounds read of a single byte in the meta encoder. This issue has been patched in versions 6.9.13-47 and 7.1.2-22.	2026-06-10	5.3	CVE-2026-45358
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-48 and 7.1.2-22, an invalid connected-components:keep-top value could result in a heap buffer over-read when performing the connected components operation. This issue has been patched in versions 6.9.13-48 and 7.1.2-22.	2026-06-10	5.7	CVE-2026-45359
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-47 and 7.1.2-22, when performing a polynomial distortion an out of bounds over-read of 24 bytes can occur when specifying specific arguments. This issue has been patched in versions 6.9.13-47 and 7.1.2-22.	2026-06-10	5.1	CVE-2026-45624
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-47 and 7.1.2-22, because of a missing check in the MNG coder it would be possible to read more images than the list limit policy would allow resulting in excessive resource use. This issue has been patched in versions 6.9.13-47 and 7.1.2-22.	2026-06-10	5.3	CVE-2026-45664
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-48 and 7.1.2-23, when using LZMA compression in the MIFF encoder an out of bounds write can occur due to a missing check. This issue has been patched in versions 6.9.13-48 and 7.1.2-23.	2026-06-10	5.5	CVE-2026-46521
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-48 and 7.1.2-23, an attacker who can connect to a magick -distribute-cache service can cause a heap buffer over-read in the server process. This issue has been patched in versions 6.9.13-48 and 7.1.2-23.	2026-06-10	5.7	CVE-2026-47166
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to version 7.1.2-24, when using an image with mask the Floyd-Steinberg dithering method it will cause a negative heap buffer over-write. This issue has been patched in version 7.1.2-24.	2026-06-10	5.5	CVE-2026-48724
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-49 and 7.1.2-24, a crafted MVG file could result in a stack overflow due to a missing depth or visited-set check. This issue has been patched in versions 6.9.13-49 and 7.1.2-24.	2026-06-10	5.5	CVE-2026-48734

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-48 and 7.1.2-24, a missing check of a return value could lead to a heap buffer over-write in the MAT decoder on 32-bit systems. This issue has been patched in versions 6.9.13-48 and 7.1.2-24.	2026-06-10	5.9	CVE-2026-48994
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-48 and 7.1.2-24, an incorrect parsing of the filename can result in a policy bypass and read files disallowed by a security policy using a symlink. This issue has been patched in versions 6.9.13-48 and 7.1.2-24.	2026-06-10	5.5	CVE-2026-49219
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-50 and 7.1.2-25, when an allocation fails in CheckPrimitiveExtent this can result in a heap-use-after-free and result in a crash. This issue has been patched in versions 6.9.13-50 and 7.1.2-25.	2026-06-10	5.9	CVE-2026-53462
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-48 and 7.1.2-23, an incorrect check in the JP2 will result in an heap buffer over-write of a single byte when specifying certain options. This issue has been patched in versions 6.9.13-48 and 7.1.2-23.	2026-06-10	4	CVE-2026-46559
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-48 and 7.1.2-23, an attacker who can connect to a magick -distribute-cache service can cause a heap buffer over-write in the server process. This issue has been patched in versions 6.9.13-48 and 7.1.2-23.	2026-06-10	4.1	CVE-2026-46692
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-48 and 7.1.2-23, an attacker who can connect to a magick -distribute-cache service can hijack a file descriptor in the server process when a race condition is met. This issue has been patched in versions 6.9.13-48 and 7.1.2-23.	2026-06-10	4.1	CVE-2026-46693
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-48 and 7.1.2-23, the distributed pixel cache was originally designed to operate without a challenge-response authentication model. This has been changed in versions 6.9.13-48 and 7.1.2-23.	2026-06-10	4.1	CVE-2026-47165
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-49 and 7.1.2-24, an infinite loop in the subimage-search operation can happen when using a crafted image. This issue has been patched in versions 6.9.13-49 and 7.1.2-24.	2026-06-10	4.7	CVE-2026-48733
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-50 and 7.1.2-25, when passing incorrect arguments in the distort operation a null pointer deference will occur. This issue has been patched in versions 6.9.13-50 and 7.1.2-25.	2026-06-10	4.3	CVE-2026-53463
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to version 7.1.2-25, when providing	2026-06-10	4	CVE-2026-53464

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	invalid options to the wand option parser a small memory leak will occur. This issue has been patched in version 7.1.2-25.			
imvks786--student_management_system	A weakness has been identified in imvks786 student_management_system up to 9599b560ad3c3b83e75d328b76bedcd489ef1f46. Affected is an unknown function of the file /add.php of the component Student Record Handler. Executing a manipulation can lead to improper access controls. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-08	6.3	CVE-2026-11532
imvks786--student_management_system	A security vulnerability has been detected in imvks786 student_management_system up to 9599b560ad3c3b83e75d328b76bedcd489ef1f46. Affected by this vulnerability is an unknown functionality of the file /see.php of the component Student Deletion Endpoint. The manipulation of the argument del leads to improper authorization. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used. This product is using a rolling release to provide continuous delivery. Therefore, no version details for affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-08	5.4	CVE-2026-11533
itsourcecode--Hospital Management System	A vulnerability was detected in itsourcecode Hospital Management System 1.0. Impacted is an unknown function of the file /adminaccount.php. The manipulation of the argument Date results in sql injection. The attack can be launched remotely. The exploit is now public and may be used.	2026-06-08	6.3	CVE-2026-11513
itsourcecode--Hospital Management System	A flaw has been found in itsourcecode Hospital Management System 1.0. The affected element is an unknown function of the file /addpatient.php. This manipulation of the argument admisiontme causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	2026-06-08	6.3	CVE-2026-11514
itsourcecode--Hospital Management System	A security vulnerability has been detected in itsourcecode Hospital Management System 1.0. This issue affects some unknown processing of the file /billing.php. The manipulation of the argument patientid leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed publicly and may be used.	2026-06-08	4.3	CVE-2026-11512
jasonpitts--WP Meta Sort Posts	The WP Meta Sort Posts plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.9. This is due to missing or incorrect nonce validation on the top-level included script in msp-options.php. This makes it possible for unauthenticated attackers to change the plugin's msp_loop_file and msp_nav_location settings via a forged request via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-09	4.3	CVE-2026-8940
jdm-labs--WP ApplicantStack Jobs Display	The WP ApplicantStack Jobs Display plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Shortcode Attributes in all versions up to, and including, 1.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with	2026-06-09	6.4	CVE-2026-8882

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.			
jelmer--dulwich	Dulwich is a pure-Python implementation of the Git file formats and protocols. Starting in version 0.1.0 and prior to version 1.2.5, a client with push access could push a tiny crafted thin pack (~174 bytes) whose delta header declares a huge dest_size. When dulwich ingested it via add_thin_pack / apply_delta, it would allocate hundreds of MB of memory based on that attacker-controlled size, with no relationship to the actual bytes received. Operators running a Dulwich-based Git server that exposes git-receive-pack (i.e. accepts pushes) - for example via dulwich.server functionality, the HTTP smart server, or anything built on ReceivePackHandler - are impacted. The issue is patched in 1.2.5. add_thin_pack now accepts a max_input_size keyword (bytes; 0/None = unlimited, matching git's semantics), and ReceivePackHandler reads receive.maxInputSize from the repository config and passes it through. Wire reads are counted and a PackInputTooLarge exception is raised once the cap is exceeded - equivalent to git index-pack --max-input-size. Users should upgrade to Dulwich 1.2.5 or later and set receive.maxInputSize in their server's repository config to a sane bound for their environment. On unpatched versions, receive.maxInputSize has no effect, so it cannot be used as a workaround. Until upgrading, operators should restrict dulwich-receive-pack (push) access to trusted, authenticated clients only, or disable it entirely on servers that only need to serve fetches and/or run the server under an OS-level memory limit (e.g. ulimit, cgroups/MemoryMax, or a container memory limit) so a malicious push is killed rather than taking down the host.	2026-06-10	5.7	CVE-2026-47734
jflyfox--jfinal_cms	A vulnerability was identified in jflyfox jfinal_cms up to 5.1.0. This impacts the function list of the file AdvicefeedbackController.java. Such manipulation of the argument orderBy leads to sql injection. The attack can be launched remotely. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-08	6.3	CVE-2026-11473
jgraph--drawio	draw.io is a configurable diagramming and whiteboarding application. Prior to version 29.7.12, a crafted .drawio file can execute arbitrary JavaScript in the editor's origin when the file is opened. The vulnerability is not in the label sanitizer (which works correctly on the rendering path) but in a feature-detection routine in the Text Format panel that reads the raw cell label and assigns it to a detached element's innerHTML without sanitization. Browsers fire onerror for failed image loads even on detached elements, so an payload in any cell label triggers script execution as soon as the cell is selected - which import does automatically. This issue has been patched in version 29.7.12.	2026-06-10	6.1	CVE-2026-46642
joshin85--Plugin Name: ePaperFlip Publisher	The ePaperFlip Publisher plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'publicationid' attribute of the `epaperflip_embed` shortcode in all versions up to, and including, 1. This is due to insufficient input sanitization and output escaping on the shortcode attribute which is injected directly into inline JavaScript. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-09	6.4	CVE-2026-7662

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kenz60--kk blog card	The kk blog card plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'blog-card' shortcode in all versions up to, and including, 1.3. This is due to insufficient input sanitization and output escaping on the shortcode's 'href' and 'type' attributes, which are concatenated directly into HTML attribute contexts in the shortcode callback registered in kk-blog-card-shortcode.php. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-09	6.4	CVE-2026-8895
koel--koel	Koel is a free, open-source music streaming solution. Prior to version 9.7.1, Koel contains a Server-Side Request Forgery (SSRF) vulnerability in the radio station creation endpoint (POST /api/radio/stations). The url field validation rules are declared without the bail keyword, so the HasAudioContentType rule - which issues HTTP requests to the supplied URL - still executes even after the SafeUrl rule has rejected the URL as pointing to a private/reserved address. Any authenticated, non-admin user can therefore coerce the server into making HEAD/GET requests to arbitrary internal hosts. This issue has been patched in version 9.7.1.	2026-06-12	6.3	CVE-2026-50552
kovidgoyal--kitty	Kitty is a cross-platform GPU based terminal. In versions prior to 0.47.2, a local privilege escalation vulnerability exists in kitty's file transmission protocol where a child process running in the terminal can write to arbitrary files on the filesystem by exploiting a TOCTOU (Time-of-Check-Time-of-Use) race condition between symlink validation and file creation. The `os.open()` call used to create files does not use `O_NOFOLLOW`, allowing an attacker to create a symlink between the initial stat check and the actual file open, causing the write to follow the symlink to an arbitrary destination. Version 0.47.2 fixes the issue.	2026-06-12	5	CVE-2026-54055
Kushan2k--student-management-system	A weakness has been identified in Kushan2k student-management-system up to f16a4ceadd6729c4b306ed4641cda3176c1ef2a. Affected by this vulnerability is the function getStatus of the file controllers/GradeController.php of the component Certificate Verification Endpoint. Executing a manipulation of the argument nic can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. This product operates on a rolling release basis, ensuring continuous delivery. Consequently, there are no version details for either affected or updated releases. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-08	6.3	CVE-2026-11475
Kushan2k--student-management-system	A security vulnerability has been detected in Kushan2k student-management-system up to f16a4ceadd6729c4b306ed4641cda3176c1ef2a. Affected by this issue is the function edit-admin of the file controllers/AdminController.php of the component Profile Update Endpoint. The manipulation of the argument isadmin leads to improper authorization. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. This product follows a rolling release approach for continuous delivery, so version details for affected or updated releases are not provided. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-08	6.3	CVE-2026-11476

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Lenovo--Application	A vulnerability was identified in the Lenovo Android Application, distributed exclusively on tablets in the Chinese market, that could allow a website visited by the built-in browser to overwrite system clipboard contents.	2026-06-10	4.3	CVE-2026-7516
Lenovo--X13 Gen 6 (Type 21RK, 21RL) Laptops (ThinkPad) BIOS	During an internal security assessment, a potential vulnerability was discovered in some ThinkPad embedded controller firmware that could allow a privileged local user to perform arbitrary reads or writes to privileged memory regions.	2026-06-10	6.7	CVE-2025-10237
Lenovo--X13 Gen 6 (Type 21RK, 21RL) Laptops (ThinkPad) BIOS	During an internal security assessment, a potential out-of-bounds write vulnerability was discovered in the BIOS of some ThinkPad products could allow a privileged local user to execute code in System Management Mode (SMM).	2026-06-10	6.7	CVE-2025-10238
Linux-PAM--Linux-PAM	Linux-PAM through 1.7.2 contains an observable timing discrepancy (CWE-208) in the pam_userdb module's plaintext-password comparison path in modules/pam_userdb/pam_userdb.c that allows a local or network-adjacent attacker able to repeatedly drive authentication through a calling service to recover the plaintext password of a target account by measuring response-timing differences. The comparison uses strncmp() (or strncasecmp() when PAM_ICASE_ARG is set) preceded by a length-equality check, so the time to reject a candidate depends on the index of the first differing byte and on whether the candidate's length matches the stored password, leaking the password length and individual prefix bytes. The vulnerable path is reached when the administrator configures pam_userdb with crypt=none, with an unrecognized crypt method, or without a crypt= argument, causing the module to store and compare credentials in plaintext.	2026-06-14	5.9	CVE-2026-54411
Ildpd--Ildpd	Ildpd is an implementation of IEEE 802.1ab (LLDP). Prior to version 1.0.22, Ildpd_decode() in src/daemon/Ildpd.c strips 802.1Q VLAN tags from received Ethernet frames by calling memmove() to shift the frame payload 4 bytes left. The third argument (byte count) is s - 2 * ETHER_ADDR_LEN but should be s - 2 * ETHER_ADDR_LEN - 4, causing a 4-byte heap buffer over-read past the malloc(h_mtu) allocation when the received frame size equals the interface MTU. This issue has been patched in version 1.0.22.	2026-06-09	6.5	CVE-2026-46433
M2Team--NanaZip	NanaZip is the 7-Zip derivative intended for the modern Windows experience. From version 3.0.1000.0 to before version 6.0.1698.0, a heap out-of-bounds read exists in the Android Verified Boot (AVB) vbmeta image parser in NanaZip (via the upstream 7-Zip AvbHandler). An unsigned integer underflow in a bounds check allows an attacker-controlled value_num_bytes field to pass validation, causing AddNameToString to read up to ~4 GiB past the end of a 64 KiB heap buffer. This causes a deterministic crash (denial of service) when opening a crafted .avb or .img file. This issue has been patched in stable version 6.0.1698.0 and preview version 6.5.1742.0.	2026-06-12	5.4	CVE-2026-47222
M2Team--NanaZip	NanaZip is the 7-Zip derivative intended for the modern Windows experience. From version 3.0.1000.0 to before version 6.0.1698.0, a heap out-of-bounds read exists in the Android Verified Boot (AVB) vbmeta image parser in NanaZip (via the upstream 7-Zip AvbHandler). A 32-bit unsigned integer overflow in the bounds check pos + ht.salt_len > descSize allows an attacker-controlled salt_len field to bypass validation, causing	2026-06-12	5.4	CVE-2026-47223

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CByteBuffer::CopyFrom to memcpy up to ~4 GiB past the end of a 64. This issue has been patched in stable version 6.0.1698.0 and preview version 6.5.1742.0.			
M2Team-- NanaZip	NanaZip is the 7-Zip derivative intended for the modern Windows experience. From version 3.0.1000.0 to before version 6.0.1698.0, a heap buffer-overflow read exists in the LVM2 physical-volume metadata parser in NanaZip (via the upstream 7-Zip LvmHandler). The vulnerability is triggered when opening a crafted LVM disk image. This issue has been patched in stable version 6.0.1698.0 and preview version 6.5.1742.0.	2026-06-12	4.3	CVE-2026-47224
MacWarrior-- clipbucket-v5	ClipBucket v5 is an open source video sharing platform. Prior to version 5.5.3 - #133, a normal authenticated user can edit another user's video subtitles because of a lack of authorization. They can upload subtitles, edit their name or delete them. This issue has been patched in version 5.5.3 - #133.	2026-06-11	6.5	CVE-2026-47238
MacWarrior-- clipbucket-v5	ClipBucket v5 is an open source video sharing platform. Prior to version 5.5.3 - #141, ClipBucket v5 contains an improper neutralization of SQL wildcard characters in the subtitle editing endpoint. An authenticated user can send a % character as the number parameter to overwrite all subtitle titles of any video they own in a single HTTP request. This issue has been patched in version 5.5.3 - #141.	2026-06-11	4.3	CVE-2026-49482
Magepeople inc.- WpEvently	Cross-Site request forgery (CSRF) vulnerability in Magepeople inc. WpEvently allows Cross Site Request Forgery. This issue affects WpEvently: from n/a through 4.1.2.	2026-06-11	4.3	CVE-2024-32110
mailerpress-- MailerPress Email Marketing, Newsletter, Email Automation & WooCommerce Emails	The MailerPress - Email Marketing, Newsletter, Email Automation & WooCommerce Emails plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Campaign HTML Content Field in all versions up to, and including, 2.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The public-facing campaign preview endpoint (/mp-email/{id}-slug/) is not affected by this vulnerability, as it applies a Content-Security-Policy header blocking all inline scripts; exploitation is limited to the admin dashboard preview.	2026-06-09	6.4	CVE-2026-8599
MariaDB--server	MariaDB server is a community developed fork of MySQL server. From versions 10.6.1 to before 10.6.26, 10.11.1 to before 10.11.17, 11.4.1 to before 11.4.11, 11.8.1 to before 11.8.7, and 12.3.1, mbstream did not check for ../ in the path when unpacking the archive. A proper backup can never contain such paths, but a specially crafted archive could have caused mbstream to create files outside of the target-dir path. This issue has been patched in versions 10.6.26, 10.11.17, 11.4.11, 11.8.7, and 12.3.2.	2026-06-12	6.3	CVE-2026-44171
MariaDB--server	MariaDB server is a community developed fork of MySQL server. From versions 10.6.1 to before 10.6.26, 10.11.1 to before 10.11.17, 11.4.1 to before 11.4.11, 11.8.1 to before 11.8.7, and 12.3.1, MariaDB allowed SELECT ... INTO OUTFILE and SELECT ... INTO DUMPFILE without verifying the FILE privilege if the FROM clause contained only subqueries. This issue has been patched in versions 10.6.26, 10.11.17, 11.4.11, 11.8.7, and 12.3.2.	2026-06-12	5	CVE-2026-44173

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
MariaDB--server	MariaDB server is a community developed fork of MySQL server. From versions 11.4.1 to before 11.4.11, 11.8.1 to before 11.8.7, and 12.3.1, a user getting EXECUTE access to a stored routine via a role, could see the routine definition even without SHOW CREATE ROUTINE privilege. This issue has been patched in versions 11.4.11, 11.8.7, and 12.3.2.	2026-06-12	4.3	CVE-2026-44169
Mattermost--Mattermost	Mattermost versions 11.6.x <= 11.6.1, 11.5.x <= 11.5.4, 10.11.x <= 10.11.15, 10.11.x <= 10.11.16 fail to require system-level permission when patching protected default system roles, which allows authenticated users with delegated user-management permissions to escalate privileges by altering built-in role permissions via the role patch API.. Mattermost Advisory ID: MMSA-2026-00656	2026-06-12	6.7	CVE-2026-6739
Mattermost--Mattermost	Mattermost versions 11.6.x <= 11.6.1, 11.5.x <= 11.5.4, 10.11.x <= 10.11.15 fail to sanitize the Remote Cluster API response on PATCH operations, which allows authenticated users with the {{manage_secure_connections}} permission to obtain remote cluster authentication tokens via a PATCH request to the remote cluster endpoint.. Mattermost Advisory ID: MMSA-2026-00662	2026-06-12	6.5	CVE-2026-7184
Mattermost--Mattermost	Mattermost versions 11.6.x <= 11.6.1, 11.5.x <= 11.5.4, 10.11.x <= 10.11.15, 10.11.x <= 10.11.16 fail to validate that a username returned during bot registration belongs to a bot account, which allows an unprivileged attacker to intercept private messages sent by plugins via direct message channels by pre-registering a user account with a predictable plugin bot username.. Mattermost Advisory ID: MMSA-2026-00649	2026-06-12	5.3	CVE-2026-6046
Mattermost--Mattermost	Mattermost versions 11.6.x <= 11.6.1, 11.5.x <= 11.5.4, 10.11.x <= 10.11.15, 10.11.x <= 10.11.16 fail to restrict role_updated websocket event broadcasts to members of the affected team or channel which allows an authenticated attacker with guest-level access to observe permission scheme change notifications for private teams they are not a member of via the websocket connection.. Mattermost Advisory ID: MMSA-2026-00616	2026-06-12	4.3	CVE-2026-3433
Mattermost--Mattermost	Mattermost versions 11.6.x <= 11.6.1, 11.5.x <= 11.5.4, 10.11.x <= 10.11.15, 10.11.x <= 10.11.16 Fail to enforce PermissionInviteUser when setting AllowOpenInvite or AllowedDomains during team creation (the check was only applied on update/patch), which allows an authenticated user holding PermissionCreateTeam but not PermissionInviteUser on the resulting team to configure invite-controlled team settings (make the team publicly joinable via open invite and/or constrain membership via allowed domains) that they are not permitted to set on an existing team via POST /api/v4/teams with allow_open_invite: true and/or a non-empty allowed_domains in the request body.. Mattermost Advisory ID: MMSA-2026-00655	2026-06-12	4.3	CVE-2026-6689
maxfoundry--WP-Paginate	WordPress Plugin WP-Paginate 2.1.3 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by manipulating the preset parameter. Attackers can submit POST requests to the plugin settings page with script payloads in the preset parameter that are stored and executed when administrators view the settings.	2026-06-08	6.4	CVE-2021-47982

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
metal3-io--ip-address-manager	IPAM is the IP address Manager for Cluster API Provider Metal3. Prior to versions 1.11.7, 1.12.4, and 1.13.0, the IPAM controller's ClusterRole granted full CRUD permissions (create, delete, get, list, patch, update, watch) on core/v1 Secrets. The controller never accesses Secrets during normal operation. If the controller pod were compromised (e.g. via supply chain attack or container escape), an attacker could leverage these excessive permissions to read, modify, or delete Secrets in the namespace, potentially exposing credentials and other sensitive data. This issue has been patched in versions 1.11.7, 1.12.4, and 1.13.0.	2026-06-12	4.4	CVE-2026-47190
Microsoft-- .NET 10.0	Improper link resolution before file access ('link following') in .NET allows an unauthorized attacker to perform tampering locally.	2026-06-09	6.2	CVE-2026-45491
Microsoft-- Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-06-09	5.5	CVE-2026-44821
Microsoft-- Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-06-09	4.7	CVE-2026-45460
Microsoft-- Microsoft Bing Search for Android	User interface (ui) misrepresentation of critical information in Microsoft Bing allows an unauthorized attacker to perform spoofing over a network.	2026-06-09	4.3	CVE-2026-45650
Microsoft-- Microsoft Defender for Endpoint for Mac	Time-of-check time-of-use (toctou) race condition in Microsoft Defender for Endpoint allows an authorized attacker to elevate privileges locally.	2026-06-09	5.5	CVE-2026-45647
Microsoft-- Microsoft Exchange Server 2016 Cumulative Update 23	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	2026-06-09	6.1	CVE-2026-45500
Microsoft-- Microsoft Exchange Server 2016 Cumulative Update 23	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	2026-06-09	6.5	CVE-2026-45501
Microsoft-- Microsoft Exchange Server 2016 Cumulative Update 23	Server-side request forgery (ssrf) in Microsoft Exchange Server allows an authorized attacker to disclose information over a network.	2026-06-09	5	CVE-2026-45502
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper limitation of a pathname to a restricted directory ('path traversal') in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-06-09	6.5	CVE-2026-45454

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	5.4	CVE-2026-33113
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	5.4	CVE-2026-45453
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	5.4	CVE-2026-45464
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	5.4	CVE-2026-45465
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	5.4	CVE-2026-47636
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	5.4	CVE-2026-47639
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	5.4	CVE-2026-48560
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	4.6	CVE-2026-45462
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	4.6	CVE-2026-45467

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	4.6	CVE-2026-45468
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	4.6	CVE-2026-45479
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office Project Server allows an authorized attacker to perform spoofing over a network.	2026-06-09	4.6	CVE-2026-45483
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	4.6	CVE-2026-47637
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	4.6	CVE-2026-47638
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	4.6	CVE-2026-47640
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	4.6	CVE-2026-47641
Microsoft-- Microsoft SharePoint Enterprise Server 2016	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-06-09	4.6	CVE-2026-48562
Microsoft--Visual Studio Code	Exposure of sensitive information to an unauthorized actor in Visual Studio Code allows an unauthorized attacker to disclose information over a network.	2026-06-09	6.5	CVE-2026-47284
Microsoft--Visual Studio Code	Relative path traversal in Visual Studio Code allows an unauthorized attacker to perform tampering over a network.	2026-06-09	6.5	CVE-2026-47287

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1607	Null pointer dereference in Windows Kerberos allows an authorized attacker to deny service over a network.	2026-06-09	6.5	CVE-2026-42903
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows DHCP Server allows an authorized attacker to disclose information locally.	2026-06-09	6.8	CVE-2026-45608
Microsoft--Windows 10 Version 1607	Protection mechanism failure in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2026-06-09	6.8	CVE-2026-50507
Microsoft--Windows 10 Version 1607	Exposure of sensitive information to an unauthorized actor in Windows NTLM allows an unauthorized attacker to perform spoofing over a network.	2026-06-09	6.5	CVE-2026-50508
Microsoft--Windows 10 Version 1607	Windows Kerberos Denial of Service Vulnerability	2026-06-09	5.3	CVE-2026-42914
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows Telephony Service allows an authorized attacker to disclose information locally.	2026-06-09	5.5	CVE-2026-42968
Microsoft--Windows 10 Version 1607	Use of uninitialized resource in Windows Push Notifications allows an authorized attacker to disclose information locally.	2026-06-09	5.5	CVE-2026-42969
Microsoft--Windows 10 Version 1607	Use of uninitialized resource in Windows Push Notifications allows an authorized attacker to disclose information locally.	2026-06-09	5.5	CVE-2026-42970
Microsoft--Windows 10 Version 1607	Use of uninitialized resource in Windows Push Notifications allows an authorized attacker to disclose information locally.	2026-06-09	5.5	CVE-2026-42971
Microsoft--Windows 10 Version 1607	Exposure of sensitive information to an unauthorized actor in Windows Hyper-V allows an authorized attacker to disclose information locally.	2026-06-09	5.5	CVE-2026-42972
Microsoft--Windows 10 Version 1607	Use of uninitialized resource in Windows Push Notifications allows an authorized attacker to disclose information locally.	2026-06-09	5.5	CVE-2026-42973
Microsoft--Windows 10 Version 1607	Exposure of sensitive information to an unauthorized actor in Windows Application Identity (AppID) Subsystem allows an authorized attacker to disclose information locally.	2026-06-09	5.5	CVE-2026-45594
Microsoft--Windows 10 Version 1607	Protection mechanism failure in Windows Mark of the Web (MOTW) allows an unauthorized attacker to bypass a security feature over a network.	2026-06-09	5.4	CVE-2026-45595
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Microsoft UxTheme Library (uxtheme.dll) allows an authorized attacker to deny service locally.	2026-06-09	5.5	CVE-2026-45606

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Microsoft--Windows 10 Version 1607	Out-of-bounds read in Windows DHCP Server allows an authorized attacker to disclose information locally.	2026-06-09	5.5	CVE-2026-45634
Microsoft--Windows 10 Version 1607	Protection mechanism failure in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2026-06-09	5.3	CVE-2026-45655
Microsoft--Windows 10 Version 1809	Exposure of sensitive information to an unauthorized actor in Windows Shell allows an authorized attacker to disclose information locally.	2026-06-09	6.5	CVE-2026-42907
Microsoft--Windows 10 Version 21H2	Exposure of sensitive information to an unauthorized actor in Windows Shell allows an authorized attacker to disclose information locally.	2026-06-09	5.5	CVE-2026-42906
Microsoft--Windows 10 Version 21H2	Incorrect calculation of buffer size in Windows TCP/IP allows an authorized attacker to deny service over an adjacent network.	2026-06-09	5.7	CVE-2026-42915
Microsoft--Windows 11 version 23H2	Out-of-bounds read in Windows Application Identity (AppID) Subsystem allows an authorized attacker to disclose information locally.	2026-06-09	5.5	CVE-2026-45604
Microsoft--Windows 11 Version 24H2	Out-of-bounds read in Windows DWM Core Library allows an authorized attacker to disclose information locally.	2026-06-09	5.5	CVE-2026-48566
Microsoft--Windows 11 version 26H1	Out-of-bounds read in Windows DWM Core Library allows an authorized attacker to disclose information locally.	2026-06-09	5.5	CVE-2026-44814
Microsoft--Windows Server 2019	Use after free in Windows Network Controller (NC) Host Agent allows an authorized attacker to deny service locally.	2026-06-09	5.5	CVE-2026-44805
moby--moby	Moby is an open source container framework. In Docker Engine prior to version 29.5.1, Docker Daemon versions 28.5.2 and prior, and Moby Daemon prior to version 2.0.0-beta.14, a race condition during docker cp mount setup allows a malicious container to create empty files or directories at arbitrary absolute paths on the host filesystem. This issue has been patched in Docker Engine version 29.5.1 and Moby Daemon version 2.0.0-beta.14.	2026-06-12	6.1	CVE-2026-41568
Mohammed-eid35--bank-management-system-springboot	A security vulnerability has been detected in Mohammed-eid35 bank-management-system-springboot up to 7b9bcc65ad7df3db29af71aed9bb500e5f24d948. This affects an unknown part of the file src/main/java/com/alien/bank/management/system/controller/TransactionController.java of the component Transaction Endpoint. Such manipulation leads to improper authorization. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. This product takes the approach of rolling releases to provide continuous delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-08	6.3	CVE-2026-11521

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
MongoDB-- MongoDB	An authenticated user with the read role may read limited amounts of uninitialized stack memory via specially-crafted issuances of the filemd5 command	2026-06-09	6.5	CVE-2026-9754
MongoDB-- MongoDB Server	A bug in query analysis processing of the \$vectorSearch aggregation stage for Queryable Encryption (QE) or Client-Side Field Level Encryption (CSFLE) results in literal values for encrypted fields within the \$vectorSearch stage filter expressions to be sent to the server as plaintext instead of ciphertext.	2026-06-09	6.5	CVE-2026-9741
MongoDB-- MongoDB Server	When using \$changestreams and \$_requestReshardingResumeToken with the exchange option the server hits an invariant which causes the server to crash. There are no special privileges needed. The user must be logged in to issue the statement.	2026-06-09	6.5	CVE-2026-9746
MongoDB-- MongoDB Server	Adding fromRouter:true and runtimeConstants.userRoles could cause aggregations to crash mongodb server.	2026-06-09	6.5	CVE-2026-9747
MongoDB-- MongoDB Server	The \$_internalConvertBucketIndexStats stage used PauseExecution as a way to signal "skip this document" when an index stats conversion failed. But PauseExecution is not a general purpose skip mechanism, but rather a TeeBuffer-internal signal used solely by \$facet to coordinate its sub-pipelines. When this stage is placed before \$facet in a pipeline, TeeBuffer receives the unexpected PauseExecution from upstream and hits a hard invariant assertion, crashing mongod.	2026-06-09	6.5	CVE-2026-9748
MongoDB-- MongoDB Server	This issue can occur when running an aggregation pipeline that uses the internal \$exchange stage configured with key-range partitioning and order-preserving delivery. If a single key range produces enough documents to fill its exchange buffer (that is, many results are routed to the same consumer), the server reaches the code path where a full per-consumer buffer is detected but the internal "high watermark" for that key range is not updated as intended.	2026-06-09	6.5	CVE-2026-9749
MongoDB-- MongoDB Server	An authenticated user can cause a MongoDB server to crash or return incorrect results by creating documents that interfere with internal metadata processing during query execution. This stems from insufficient separation between user-controlled document fields and internal metadata in certain execution paths.	2026-06-09	6.5	CVE-2026-9750
MongoDB-- MongoDB Server	An authorized user could trigger a server crash by running a query with a 2dsphere index on a field that stores a GeoJSON GeometryCollection containing a Polygon with a strict-winding CRS. Strict-winding polygons are intentionally unsupported for indexing, but the guard that rejects them does not inspect members of a GeometryCollection, allowing the unsafe path to be reached which ends with an ensuing null-pointer dereference.	2026-06-09	6.5	CVE-2026-9752
MongoDB-- MongoDB Server	MongoDB server may log authentication parameters, including credentials, to the server log during SASL authentication. When connection health metric logging is enabled, the full authentication parameters are written to the log without redaction.	2026-06-09	5.5	CVE-2026-9735
MongoDB-- MongoDB Server	The ldapQueryPassword parameter, when set through the runtime setParameter command, will log the new password to the mongod.log file in plain text.	2026-06-09	5.5	CVE-2026-9751

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
MongoDB--MongoDB server	In MongoDB Server 8.0, an aggregation stage can leave its _subPipeline field null during processing of certain pipelines. If a getMore is subsequently issued on the same cursor, the server may dereference this null sub-pipeline when reattaching to the operation context, accessing an invalid address and crashing the process. This issue allows an authenticated user who can run aggregation pipelines to cause a denial of service by issuing a specially crafted aggregation followed by getMore on affected versions.	2026-06-09	6.5	CVE-2026-9743
Moovit--Bus & Public Transit App	A flaw has been found in Moovit Bus & Public Transit App 1.18 on Android. This affects an unknown part of the component com.tranzmate. Executing a manipulation can lead to improper authorization in handler for custom url scheme. The attack can only be executed locally. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-14	5.3	CVE-2026-12189
mra13--Accept Stripe Payments	WordPress Plugin Stripe Payments 2.0.39 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts through the AcceptStripePayments-settings[currency_code] parameter. Attackers can submit POST requests to /wp-admin/options.php with script payloads in the currency_code field to execute arbitrary JavaScript in administrator browsers when settings are viewed.	2026-06-08	6.4	CVE-2021-47983
myasui--WP Vault	WP Vault 0.8.6.6 contains a local file inclusion vulnerability that allows unauthenticated attackers to read arbitrary files by exploiting an unescaped parameter in the include functionality. Attackers can supply directory traversal sequences through the wpv-image GET parameter to access sensitive files like system configuration and credentials.	2026-06-09	6.2	CVE-2016-20064
nationalsecurityagency--ghidra	Ghidra before 12.1 contains a heap-use-after-free vulnerability in SleighBuilder::generatePointerAdd caused by iterator invalidation when PcodeCacher::allocateInstruction reallocates the issued vector. Attackers can trigger memory corruption by decompiling malicious binaries through the public Sleigh::oneInstruction C++ API, affecting downstream SLEIGH library consumers.	2026-06-10	6.1	CVE-2026-49496
nationalsecurityagency--ghidra	Ghidra 10.2 before 12.1 contains an uncontrolled resource consumption vulnerability in ExportTrie.parseTrie() that lacks cycle detection when traversing Mach-O binary export tries. A crafted Mach-O binary with circular references in the export trie causes unbounded queue growth and exponential string concatenation, triggering OutOfMemoryError that crashes the entire JVM and loses all unsaved work.	2026-06-10	5.5	CVE-2026-49495
nationalsecurityagency--ghidra	Ghidra before 12.0.3 contains an out-of-memory vulnerability in the rust_demangle function that allocates unbounded output buffers without size limits. Attackers can craft malicious Rust symbol names in binaries to trigger exponential memory allocation, causing process crashes during binary analysis.	2026-06-10	5.5	CVE-2026-52753
nationalsecurityagency--ghidra	Ghidra before 12.2 contains an unauthenticated path traversal vulnerability in the IsfServer that accepts TCP connections and passes client-supplied namespace strings directly to filesystem operations without validation. Remote attackers can connect to port 54321 and send crafted	2026-06-10	4.8	CVE-2026-52756

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	protobuf messages with traversal sequences to enumerate filesystem paths and probe arbitrary files.			
nationalsecurityagency--ghidra	Ghidra before 12.1 contains a heap-use-after-free vulnerability in the decompiler's HighVariable::merge() function during the variable merging pass. Attackers can trigger this vulnerability by crafting a binary that causes stale pointers in the HighIntersectTest::highedgemap cache to be dereferenced, reading and writing the flags field of freed heap memory when a user opens the binary in Ghidra's decompiler view.	2026-06-10	4.4	CVE-2026-52757
Naxclow--Smart Doorbell X3	Naxclow device identifiers use fixed manufacturing prefixes combined with sequential counters, producing a fully predictable and enumerable identifier space. Because the platform also exposes an endpoint that reveals the current identifier high-water mark, the active fleet can be enumerated.	2026-06-12	5.3	CVE-2026-42932
Naxclow--Smart Doorbell X3	The Naxclow platform exposes a registration endpoint that accepts signed requests containing a batch prefix and an arbitrary caller-supplied account identifier, without validating any ownership relationship. Each call mints a new sequential device identifier and returns the current high-water counter value for the batch, allowing callers to measure and enumerate the active device space. The endpoint's behavior enables precise fleet enumeration.	2026-06-12	5.3	CVE-2026-50244
Naxclow--Smart Doorbell X3	During WiFi association, Naxclow device firmware prints the host network's SSID, PSK, and negotiated WPA keys in cleartext to an exposed UART console on production hardware. The UART pads are labeled, run with default serial settings, and drop to an interactive RT-Thread shell that permits arbitrary memory reads, enabling full firmware extraction. An attacker with brief physical access, common for outdoor-mounted devices, can therefore recover WiFi credentials and bootstrap firmware-side attacks.	2026-06-12	4.6	CVE-2026-50099
Neovim--Neovim	A flaw has been found in Neovim up to 0.12.2. Affected by this issue is the function M.read of the file runtime/lua/vim/secure.lua of the component View Branch. Executing a manipulation of the argument path can lead to command injection. It is possible to launch the attack on the local host. The exploit has been published and may be used. This patch is called f83e0dcdf8cf18de94828341b0a1a61a86c75baf. A patch should be applied to remediate this issue.	2026-06-08	5.3	CVE-2026-11487
nesquena--hermes-webui	Hermes WebUI before version 0.51.269 contains a profile isolation bypass vulnerability that allows authenticated users to access data belonging to other profiles by querying the session search endpoint without active-profile filtering. Attackers can send requests to the sessions search handler to retrieve session titles and transcript message content from profiles other than their own active profile.	2026-06-09	6.5	CVE-2026-49956
nesquena--hermes-webui	Hermes WebUI before version 0.51.270 contains a resource exhaustion vulnerability that allows unauthenticated remote attackers to degrade service availability by repeatedly calling the passkey options endpoint without completing assertion. Attackers can send unlimited POST requests to the authentication endpoint, causing unbounded growth of the challenge store file and excessive CPU and disk I/O through repeated JSON file rewrites.	2026-06-09	5.3	CVE-2026-49955

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nesquena--hermes-webui	Hermes WebUI before version 0.51.303 contains a time-of-check time-of-use (TOCTOU) race condition vulnerability in the git_discard function within api/workspace_git.py that allows attackers to delete files outside the configured workspace boundary by replacing a validated path component with a symlink after validation but before deletion. Attackers can substitute a workspace-controlled path component with a symlink pointing to an external directory between the safe_resolve_ws() validation step and the subsequent Path.unlink() or shutil.rmtree() deletion call, causing the delete operation to follow the symlink and remove arbitrary files outside the workspace.	2026-06-09	5	CVE-2026-49958
netty--netty	Netty is a network application framework for development of protocol servers and clients. Prior to versions 4.1.135.Final and 4.2.15.Final, Netty's DNS resolver uses a predictable PRNG for generating DNS transaction IDs and defaults to a static UDP source port. This combination reduces the entropy of DNS queries, enabling DNS Cache Poisoning (Kaminsky attack). Versions 4.1.135.Final and 4.2.15.Final patch the issue.	2026-06-12	6.8	CVE-2026-45673
netty--netty	Netty is a network application framework for development of protocol servers and clients. Prior to versions 4.1.135.Final and 4.2.15.Final, DefaultHttp2Connection.DefaultEndpoint initialises maxActiveStreams/maxStreams to Integer.MAX_VALUE, and Http2Settings never inserts SETTINGS_MAX_CONCURRENT_STREAMS by default (Http2Settings.java:305-307 only clamps a user-supplied value). Unless the application explicitly calls initialSettings().maxConcurrentStreams(n), a Netty HTTP/2 server advertises no limit and enforces none locally. Each open stream allocates a DefaultStream object, PropertyMap slots, flow-controller state and IntObjectHashMap entry; with ~2^30 permissible odd stream IDs a single TCP connection can create hundreds of thousands of long-lived stream objects. This is also the precondition for CVE-2023-44487-style Rapid-Reset amplification, where the absence of a low concurrent cap multiplies backend work. Versions 4.1.135.Final and 4.2.15.Final patch the issue.	2026-06-12	5.3	CVE-2026-47244
netty--netty	Netty is a network application framework for development of protocol servers and clients. In netty-codec-http2 prior to versions 4.1.135.Final and 4.2.15.Final, the `DelegatingDecompressorFrameListener` class orchestrates HTTP/2 decompression by embedding a per-stream `EmbeddedChannel` that runs the appropriate decompression codec (gzip, deflate, zstd) and forwards decompressed chunks to a wrapped listener. Each decompressed chunk is a pooled `ByteBuf` handed to an anonymous `ChannelInboundHandlerAdapter` tail handler, which becomes the sole owner responsible for releasing it. A remote peer could send frames that would result in the flow-controller throwing and so trigger a resource leak which at the end might take down the whole JVM due OOME. Versions 4.1.135.Final and 4.2.15.Final patch the issue.	2026-06-12	5.3	CVE-2026-48043
netty--netty	Netty is a network application framework for development of protocol servers and clients. Prior to versions 4.1.135.Final and 4.2.15.Final, before reading the first request-line, `HttpObjectDecoder` skips every byte for which `Character.isISOControl(b)` is `true` (0x00-0x1F and 0x7F) as well as all whitespace. RFC 9112 §2.2 only asks servers to ignore empty CRLF lines preceding the request-line - a carefully scoped robustness allowance intended to handle HTTP/1.0 POST workarounds. Silently absorbing NUL bytes, SOH, STX, and other non-CRLF control characters goes significantly	2026-06-12	5.3	CVE-2026-50020

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	beyond this, and can be exploited for request-boundary confusion in pipelined or multiplexed transports where a front-end component treats those bytes differently. Versions 4.1.135.Final and 4.2.15.Final patch the issue.			
netty--netty	Netty is a network application framework for development of protocol servers and clients. Prior to versions 4.1.135.Final and 4.2.15.Final, <code>netty_unix_socket_recvFd</code> sets <code>msg_control</code> to <code>`char control[MSG_SPACE(sizeof(int))`](line 940) - 24 bytes on 64-bit Linux. A peer-sent <code>SCM_RIGHTS</code> <code>msg</code> carrying two ints has <code>msg_len = MSG_LEN(8) = 24</code>, which fits exactly with no <code>MSG_CTRUNC</code>, so the kernel installs both fds in the receiving process. The subsequent check <code>`msg->msg_len == MSG_LEN(sizeof(int))`](line 972, expected 20) fails, the branch that would read the fd is skipped, and neither installed fd is closed. The <code>for(;;)</code> loop calls <code>recvmsg</code> again (non-blocking <code>â†’ EAGAIN â†’</code> Java maps to 0 <code>â†’</code> read loop exits normally), leaving two leaked fds per message. There is no <code>MSG_CTRUNC</code> handling. Reachable via <code>Epoll/KQueue DomainSocketChannel</code> when the application opts into <code>DomainSocketReadMode.FILE_DESCRIPTOR</code> (non-default). Versions 4.1.135.Final and 4.2.15.Final patch the issue.</code></code>	2026-06-12	4	CVE-2026-45536
netty--netty	Netty is a network application framework for development of protocol servers and clients. Prior to version 4.2.15.Final, Netty QUIC exposes the stateless reset token on the network path when using the default HMAC-based connection-ID and stateless-reset-token generators. The reset token for the server's current source connection ID can be derived from bytes that appear as the connection ID in QUIC headers after a source-CID rotation. An on-path attacker observing the headers can use the token to perform a Denial of Service by sending a spoofed Stateless Reset packet. Version 4.2.15.Final patches the issue.	2026-06-12	4.8	CVE-2026-50009
nezhaq--nezha	Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. From version 1.4.0 to before version 2.0.9, any authenticated non-admin member can connect to the server-status WebSocket and receive telemetry for all servers, including servers owned by other users. The normal server list API filters objects by <code>HasPermission</code> , but the WebSocket stream treats the presence of any authenticated user as authorization for the full unfiltered server list. This issue has been patched in version 2.0.9.	2026-06-12	6.5	CVE-2026-47124
nezhaq--nezha	Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. From version 0.20.0 to before version 2.0.10, an authenticated Nezha dashboard user can create or update a DDNS profile with provider webhook and configure an arbitrary <code>webhook_url</code> , HTTP method, request body, and headers. When DDNS is triggered for a server that uses that profile, the dashboard process sends the configured request with <code>utils.HttpClient</code> without the SSRF protections used by notification webhooks. This allows a low-privileged authenticated user who controls an owned server/DDNS profile to make the dashboard host issue HTTP requests to loopback or internal network services. The response body is not returned to the attacker in the confirmed path, so this is a blind SSRF / internal state-changing request primitive. This issue has been patched in version 2.0.10.	2026-06-12	6.4	CVE-2026-47268

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nezhahq--nezha	Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. From version 2.0.14 to before version 2.1.0, authenticated users can claim the dashboard Host through NAT and preempt all dashboard routing. This issue has been patched in version 2.1.0.	2026-06-12	6.5	CVE-2026-53520
nezhahq--nezha	Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. From version 2.0.14 to before version 2.1.0, PATCH /server/{id} accepts and persists nonexistent ddns_profiles IDs for a member-owned server. If another user later creates a DDNS profile with one of those IDs, the DDNS worker resolves the stored ID and dispatches an update using the other user's DDNS profile configuration in the context of the attacker's server. This issue has been patched in version 2.1.0.	2026-06-12	6.4	CVE-2026-53521
nezhahq--nezha	Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. From version 1.0.0 to before version 2.2.0, the Nezha dashboard exposes two endpoints that create long-lived WebSocket streams to monitored agents: POST /api/v1/terminal â createTerminal() (terminal.go:27-67) and POST /api/v1/file â createFM() (fm.go:28-67). Both call rpc.NezhaHandlerSingleton.CreateStream(streamId, ...) which inserts a new ioStreamContext into an unbounded map[string]*ioStreamContext (s.ioStreams in io_stream.go:59-67). There is no per-user rate limit, no global semaphore, and no per-server connection cap. This issue has been patched in version 2.2.0.	2026-06-12	6.5	CVE-2026-53522
nezhahq--nezha	Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. From version 1.0.0 to before version 2.2.0, the getRedirectURL function in oauth2.go:22-29 constructs the OAuth2 callback URL by concatenating the request's Host header with a fixed path, with zero validation of the Host header. This can result in host header injection. This issue has been patched in version 2.2.0.	2026-06-12	6.8	CVE-2026-53523
nezhahq--nezha	Nezha Monitoring is a self-hostable, lightweight, servers and websites monitoring and O&M tool. From version 2.0.0 to before version 2.0.14, private services ('EnableShowInService: false') are enumerable via per-server endpoints, leaking name and timing data. This issue has been patched in version 2.0.14.	2026-06-12	5.3	CVE-2026-49397
nimiq--core-rs-albatross	Nimiq is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. Prior to version 1.4.0, when LightBlockchain::rebranch() adopts a fork chain whose tip is a macro block (checkpoint or election), it only updates self.head but fails to update self.macro_head, self.election_head, self.current_validators, or store the election header in the chain_store. This is in direct contrast with the full Blockchain::rebranch() at blockchain/src/blockchain/push.rs:504-518, which correctly updates all macro/election state when the new head is a macro block. After a rebranch to a macro block, the stale macro_head causes subsequent macro blocks pushed via push() to be verified against the wrong predecessor via verify_macro_successor(&this.macro_head). If the rebranch target was an election block, the stale current_validators causes every subsequent block to fail verify_validators(), completely stalling the light client's chain progression. This issue has been patched in version 1.4.0.	2026-06-09	6.5	CVE-2026-46540

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nimiq--core-rs-albatross	Nimiq is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. network-libp2p handles kad get-record query progress in handle_dht_get (network-libp2p/src/swarm.rs). Prior to version 1.4.0, when a peer returns a FoundRecord, the code verifies the record via dht_verifier.verify(&record.record). On verifier error, handle_dht_get logs and returns early without completing the oneshot used by Network::dht_get, and without cleaning up per-query bookkeeping. Later query progress can hit the "DHT inconsistent state" path and also return without cleanup. Because Network::dht_get awaits the oneshot without a timeout, the caller future can hang indefinitely. This issue has been patched in version 1.4.0.	2026-06-09	5.3	CVE-2026-44505
nimiq--core-rs-albatross	Nimiq is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. Prior to version 1.4.0, a logic flaw in BlockInclusionProof::is_block_proven causes the function to return true without performing any cryptographic verification when get_interlink_hops yields an empty hop list. This occurs when the target block is at the election block position immediately preceding the election head's epoch. An attacker providing transaction inclusion proofs can forge a MacroBlock header for that epoch position and have it accepted as "proven" without any hash or signature verification. This issue has been patched in version 1.4.0.	2026-06-09	5.9	CVE-2026-46539
nimiq--core-rs-albatross	Nimiq is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. Prior to version 1.5.0, a remote peer can crash any full node by sending a RequestBatchSet message containing the genesis block's hash. The handler calls get_epoch_chunks which iterates backwards through macro blocks using Policy::macro_block_before. When it reaches the genesis block number, macro_block_before panics with "No macro blocks before genesis block". This issue has been patched in version 1.5.0.	2026-06-09	5.3	CVE-2026-46543
nimiq--core-rs-albatross	Nimiq is a Rust implementation of the Nimiq Proof-of-Stake protocol based on the Albatross consensus algorithm. Prior to version 1.4.0, a denial-of-service vulnerability exists in the Ed25519 multisig delinearization code path. Ed25519PublicKey::delinearize() in keys/src/multisig/mod.rs called .unwrap() on curve point decompression, which panics when a public key is constructed from 32 bytes that do not represent a valid point on the Ed25519 curve. Ed25519PublicKey construction only validates byte length, not curve membership, so invalid keys can reach the delinearization path and crash the hosting process. This issue has been patched in version 1.4.0.	2026-06-09	4.3	CVE-2026-46542
OfflineIMAP--OfflineIMAP	OfflineIMAP before 8.0.3 trusts the server with their STARTTLS capability prior to authentication, which allows STRIPTLS/man-in-the-middle attacks, taking over the connection and extracting account credentials in cleartext.	2026-06-08	6.5	CVE-2020-37248
open-telemetry--opentelemetry-cpp	OpenTelemetry-cpp is the C++ implementation of OpenTelemetry. Prior to release 1.27.0, the OTLP HTTP exporters (traces/metrics/logs) read the full HTTP response into an in-memory vector of bytes without a size cap. This is exploitable for memory exhaustion when the configured collector endpoint is attacker-controlled (or a network attacker can MITM the exporter connection). This vulnerability is fixed in opentelemetry-cpp release 1.27.0.	2026-06-12	5.3	CVE-2026-44967

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openbullet--openbullet2	OpenBullet2 through version 0.3.2 on Windows contains a credential disclosure vulnerability that allows remote attackers to capture the NTLMv2 hash of the process user by configuring a job proxy source with a UNC path pointing to an attacker-controlled server. When the job starts, the application attempts to load proxies from the UNC path, triggering an SMB authentication attempt that discloses the NTLMv2 hash, which can then be relayed or cracked offline.	2026-06-08	6.5	CVE-2026-39908
OpenClaw--OpenClaw	OpenClaw before 2026.5.6 contains an approval policy bypass vulnerability in the Skill Workshop apply flow that allows agent tool calls to set apply: true despite approvalPolicy: pending configuration. Attackers can exploit this by reaching the affected apply path to apply workshop changes before the expected approval step, potentially modifying configurations without proper authorization.	2026-06-11	6.5	CVE-2026-53808
OpenClaw--OpenClaw	OpenClaw before 2026.5.19 contains an authorization bypass vulnerability in message read actions that skips channel allowlist checks. Lower-trust callers can request messages from channels not intended for them by exploiting insufficient validation in the affected feature, potentially exposing sensitive channel messages.	2026-06-11	6.5	CVE-2026-53815
OpenClaw--OpenClaw	OpenClaw before 2026.4.24 contains an authorization bypass vulnerability in the MCP loopback feature that allows non-owner callers to skip owner-only tool policies and before-tool-call hooks. Attackers can invoke owner-only behavior through the affected loopback path to execute restricted tools when the feature is enabled and reachable.	2026-06-11	6.6	CVE-2026-53818
OpenClaw--OpenClaw	OpenClaw before 2026.5.12 contains an exec denylist bypass vulnerability in the bundle MCP loopback session-spawn path that allows authenticated callers to bypass intended command restrictions. Attackers can reach the affected bundled MCP session-spawn path to start sessions with broader command reach than intended.	2026-06-12	6.6	CVE-2026-53820
OpenClaw--OpenClaw	OpenClaw before 2026.4.24 contains a token revocation vulnerability allowing callers with revoked slash tokens to continue executing commands during monitor refresh windows. Attackers can exploit stale token acceptance to invoke slash command behavior briefly after token revocation, potentially executing unauthorized actions depending on operator configuration.	2026-06-12	6.5	CVE-2026-53824
OpenClaw--OpenClaw	OpenClaw before 2026.4.7 contains an arbitrary file read vulnerability in the memory-wiki ingest feature that allows authenticated Gateway operators with operator.write scope to read local files outside intended ingest sources. Attackers with operator.write access can specify arbitrary local file paths to import file content into wiki memory, bypassing access restrictions.	2026-06-12	6.5	CVE-2026-53825
OpenClaw--OpenClaw	OpenClaw before 2026.5.2 contains a credential exposure vulnerability in message.action forwarding that allows model-controlled metadata to forward action payloads with Gateway credentials to attacker-supplied loopback URLs. Remote attackers can intercept Gateway tokens and action payloads by providing malicious loopback targets through model-controlled action metadata.	2026-06-12	6.5	CVE-2026-53827

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
OpenClaw-- OpenClaw	OpenClaw before 2026.4.22 contains a webhook secret revocation bypass vulnerability allowing callers with old Slack and Zalo webhook secrets to remain active after secrets.reload. Attackers can exploit the stale-secret window to deliver webhook events after operator-expected secret revocation, potentially accepting previous credentials.	2026-06-12	6.5	CVE-2026-53830
OpenClaw-- OpenClaw	OpenClaw before 2026.5.7 contains a hostname validation vulnerability in retry endpoint checks that allows matching hostname prefixes instead of exact hostnames. Attackers can exploit this by crafting a hostname prefix resembling a trusted host to send authentication material to untrusted endpoints.	2026-06-12	6.5	CVE-2026-53839
OpenClaw-- OpenClaw	OpenClaw before 2026.4.26 contains an information disclosure vulnerability in sandboxed session spawning that exposes the real workspace path to child prompts. Attackers can exploit this by spawning child sessions from sandboxed parents to reveal host workspace location or related memory context to child models.	2026-06-12	4.3	CVE-2026-53826
OpenClaw-- OpenClaw	OpenClaw before 2026.5.6 contains a configuration enforcement bypass vulnerability in Feishu dynamic-agent bindings that allows authenticated senders to create or update bindings without honoring configured config-write controls. Attackers can exploit this by leveraging the dynamic-agent binding feature to change sender-agent binding state beyond intended policy, potentially enabling unauthorized binding modifications.	2026-06-12	4.3	CVE-2026-53835
openfga-- openfga	OpenFGA is an authorization/permission engine built for developers. Prior to version 1.16.0, when iterator caching is enabled, two distinct check requests can produce the same cache key, leading to OpenFGA reusing an earlier cached result for a subsequent request. This issue has been patched in version 1.16.0.	2026-06-10	5	CVE-2026-48096
OpenStack-- Ironic	In OpenStack Ironic through 35.0.1, when applying a PATCH to update fields in volume properties the user is authorized for, Ironic can return unredacted sensitive information (such as iSCSI credentials). The PATCH outcome is a security issue; the POST outcome is not a security issue.	2026-06-14	6.8	CVE-2026-54421
pickplugins-- Accordions	The Accordions plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Accordion body field in all versions up to, and including, 2.3.23 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Custom-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-09	6.4	CVE-2026-10862
QEMU--Virtio-blk	A flaw was found in QEMU's virtio-blk device. The issue arises because the device does not properly validate the size of input descriptors before writing data. A malicious guest with high privileges could exploit this vulnerability by submitting a malformed virtio-blk SCSI request, leading to an out-of-bounds write in the host heap memory and a potential denial of service (DoS) for the QEMU process.	2026-06-12	6.7	CVE-2026-48914
QloApps-- QloApps	QloApps through 1.7.0 contains a stored cross-site scripting vulnerability in the admin file manager that allows authenticated administrators to inject malicious JavaScript by uploading crafted SVG files. Attackers can embed JavaScript event handlers such as onload within SVG files uploaded	2026-06-08	4.8	CVE-2026-25558

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	through the file manager to execute arbitrary scripts in the browser of any user who subsequently views the file.			
quantumcloud--Simple Link Directory	Simple Link Directory through 9.0.4 interpolates the sld_no_results_found option into a JavaScript string literal without encoding. Because sanitize_text_field leaves quotes intact, a stored payload breaks out of the string and runs script for every page visitor.	2026-06-10	5.4	CVE-2026-53741
quantumcloud--Simple Link Directory	Simple Link Directory through 9.0.4 echoes embed shortcode attributes into HTML data attributes without escaping in the embedder template. Attackers with contributor access can craft a shortcode attribute that injects an event handler executing in a viewer's browser.	2026-06-10	5.4	CVE-2026-53742
rahulbhargale--WP Emoticon Rating	The WP Emoticon Rating plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.1. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-09	6.1	CVE-2026-8910
rahulbhargale--WP-Ultimate-Map	The WP-Ultimate-Map plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1. This is due to missing nonce validation on the process_init() function hooked to admin_init, which saves plugin settings (zoom-level, focus-lat, focus-lng, sel_places, sel_routes) via update_option() based solely on the presence of a save-setting POST parameter. Additionally, the saved values - particularly zoom-level - are stored without sanitization and later echoed into an HTML attribute (and inline JavaScript) on the settings page without escaping. This makes it possible for unauthenticated attackers to change plugin settings and inject arbitrary web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-09	6.1	CVE-2026-8907
rahulbhargale--WpMobi	The WpMobi plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.0.3. This is due to missing or incorrect nonce validation on the handleSaveGeneralSettings function. This makes it possible for unauthenticated attackers to modify the plugin's General Settings and inject arbitrary web scripts into the administrator's browser via the unescaped app_name attribute reflection via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. The injected script executes even when the supplied app_name value fails validation and is not persisted to the database, because the form is re-rendered with the attacker-supplied in-memory value on validation failure.	2026-06-09	4.3	CVE-2026-8909
Red Hat--Red Hat Ansible Automation Platform 2	A path traversal vulnerability was found in awxkit, the CLI tool for AWX. The YAML !include directive does not sanitize file paths, allowing an attacker to craft a malicious YAML file that reads arbitrary YAML-formatted files from the local filesystem when a user imports it using "awx --conf.format yaml import". This is a client-side vulnerability requiring user interaction.	2026-06-09	4.7	CVE-2026-52902
Red Hat--Red Hat Build of Keycloak	A flaw was found in the admin-ui-ext component of Keycloak, which provides extended administrative user interface capabilities. The issue occurs because certain bulk role-removal endpoints fail to perform granular permission checks when deleting role mappings. This allows a delegated administrator with limited permissions to remove highly	2026-06-11	4.9	CVE-2026-11986

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	privileged roles from other users or groups, potentially disrupting administrative access control.			
Red Hat--Red Hat Directory Server 11	A flaw was found in 389 Directory Server. The Content Synchronization persistent search plugin allows unbounded memory growth when an authenticated client stops reading sync responses, enabling denial of service. Additional race conditions in plugin thread lifecycle can cause crashes during connection teardown or shutdown.	2026-06-08	6.5	CVE-2026-11611
Red Hat--Red Hat Directory Server 11	A heap buffer overflow flaw was found in 389 Directory Server. When serializing objectclass definitions, the oc_superior (SUP) field length is omitted from buffer size calculations in read_schema_dse() and schema_oc_to_string(), but the field is still written via strcat(). An attacker with Directory Manager privileges, or a compromised replication supplier, can trigger a server crash by creating objectclasses with long SUP values. This is an incomplete fix variant of CVE-2025-14905.	2026-06-10	6.5	CVE-2026-11884
Red Hat--Red Hat Directory Server 11	A flaw was found in 389 Directory Server. The ldap_utf8prev() function reads bytes before the start of a buffer without bounds checking, causing a heap buffer over-read in string filter parsing that may influence internal filter processing behavior.	2026-06-09	5	CVE-2026-11787
Red Hat--Red Hat Directory Server 11	A flaw was found in 389 Directory Server. The dereference control plugin does not check for allocation failure before using a BER structure, allowing an unauthenticated remote attacker to crash the LDAP server when the system is under memory pressure.	2026-06-09	5.9	CVE-2026-11788
Red Hat--Red Hat Directory Server 11	A flaw was found in 389 Directory Server. A type confusion in the SSO token extended operation handler causes partial stack address information to be disclosed in LDAP responses to authenticated users.	2026-06-09	4.3	CVE-2026-11785
Red Hat--Red Hat Directory Server 11	A flaw was found in 389 Directory Server. The SMD5 password storage plugin performs unsigned integer underflow when computing salt length from a crafted password hash shorter than 16 bytes, causing a buffer over-read that crashes the LDAP server during authentication.	2026-06-09	4.9	CVE-2026-11789
Red Hat--Red Hat Directory Server 11	A flaw was found in 389 Directory Server. The PBKDF2-SHA256 password storage plugin does not enforce an upper bound on the iteration count extracted from stored password hashes. A privileged attacker who can modify a user's password hash can cause excessive CPU consumption during authentication, resulting in denial of service.	2026-06-09	4.9	CVE-2026-11790
Red Hat--Red Hat Directory Server 11	A stack buffer overflow flaw was found in 389 Directory Server. The checkPrefix() function in pw.c copies an attacker-controlled algorithm ID into a 256-byte stack buffer without bounds checking when parsing reversible-encrypted attribute values. An attacker with Directory Manager privileges can crash the LDAP server by storing a crafted credential with an oversized algorithm ID. FORTIFY_SOURCE mitigates this to denial of service only.	2026-06-09	4.9	CVE-2026-11793
Red Hat--Red Hat Enterprise Linux 10	An out-of-bounds write vulnerability was found in GStreamer's H.266/VVC PPS picture partition parser in gst-plugins-bad. In the multi-slice-in-tile processing of gst_h266_parser_parse_picture_partition() (gst_h266parser.c), the loop iterates without checking that the slice index stays within bounds, writing past three fixed-size arrays (slice_height_in_ctus, slice_top_left_ctu_x, slice_top_left_ctu_y) in the	2026-06-11	6.5	CVE-2026-53701

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	GstH266PPS structure. While the initial proof-of-concept demonstrated a 4-byte out-of-bounds write, the code permits larger writes across multiple iterations. A crafted H.266/VVC media file can trigger this vulnerability.			
Red Hat--Red Hat Enterprise Linux 10	A stack buffer overflow flaw was found in the GStreamer H.265 codec parser library (gst-plugins-bad). When parsing a buffering period SEI message, the parser uses an incorrect loop bound derived from cpb_cnt_minus1[i] (the loop index) instead of the sub-layer 0 CPB count cpb_cnt_minus1[0] from the referenced Sequence Parameter Set. A crafted H.265 video file or stream can cause the parser to write beyond the bounds of stack-allocated CPB delay arrays, resulting in a crash or potential stack memory corruption.	2026-06-11	6.5	CVE-2026-53702
Red Hat--Red Hat Enterprise Linux 6	A content injection vulnerability was found in the ABRT post-create event handler scripts in libreport. The event script queries the systemd journal for log entries matching the crashed process and writes the results to files in the dump directory without sanitizing embedded control characters. A local user can inject arbitrary content into the journal output by embedding newline characters in syslog messages, controlling the content that root writes to dump directory files.	2026-06-13	5.5	CVE-2026-54231
Red Hat--Red Hat Hardened Images	An integer underflow vulnerability was found in MIT krb5 in the berval2tl_data() function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c. The function performs an unsigned subtraction (bv_len - 2) without a prior bounds check. When bv_len is 0 or 1, the subtraction wraps to a large value which is then truncated to uint16_t, yielding 0xFFFFE (65534) or 0xFFFF (65535). The subsequent malloc succeeds and memcpy reads up to 65534 bytes from a 0-1 byte buffer, resulting in a heap out-of-bounds read. The attack vector involves a malicious or compromised LDAP KDB backend returning a krbExtraData attribute with bv_len < 2, triggering the underflow when the KDC or kadmind reads principal data.	2026-06-11	5	CVE-2026-11850
Red Hat--Red Hat Quay 3	A flaw was found in Quay. The filedrop endpoint accepts any mime type without validation, allowing an authenticated user with repository write access to upload a malicious SVG file containing JavaScript. The file is stored and served inline through the CDN, enabling stored cross-site scripting when a victim visits the archive URL.	2026-06-08	5.4	CVE-2026-11569
Revolution Slider--Slider Revolution	The Slider Revolution plugin for WordPress is vulnerable to Sensitive Information Disclosure in versions up to and including 7.0.10. This is due to three compounding design flaws: (1) the plugin leaks a valid backend AJAX nonce (revslider_actions) to all authenticated users including Subscribers via the admin_footer hook; (2) the wordpress.create_image_from_url action is explicitly allowlisted in the \$user_allowed array, bypassing the administrator-only access control; (3) the create_wordpress_image_from_url() function accepts an attacker-controlled url parameter that is passed to import_media(), where path_or_url_exists() explicitly accepts local filesystem paths (file_exists() && is_readable()) with no restriction to remote HTTP/HTTPS URLs, and @copy() physically copies those files into the publicly accessible /wp-content/uploads/revslider/ai/ directory. The MIME type check trusts the attacker-supplied content_type parameter to derive the destination extension without verifying actual file content, and the source extension blacklist does not block many sensitive types (.sql, .log, .json, .bak, .xml,	2026-06-09	6.5	CVE-2026-7542

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	.csv, .conf, .yaml, .yml, .pem, .key, .crt, .txt, .db, etc.). This makes it possible for authenticated attackers with Subscriber-level access and above to read the contents of server files with non-blacklisted extensions by having them copied to a publicly accessible URL.			
rikoyoz--bit7z	bit7z is a cross-platform C++ static library that allows the compression/extraction of archive files. Prior to version 4.0.12, there is an arbitrary file overwrite vulnerability via symlink attack on predictable temp files during archive update. This issue has been patched in version 4.0.12.	2026-06-10	6.1	CVE-2026-45384
romancartsupport--RomanCart Ecommerce	The RomanCart Ecommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'bclass' attribute (and other attributes) of the romancart_button shortcode in versions up to, and including, 2.0.8. This is due to insufficient input sanitization and output escaping on user supplied attributes within the romancart_button_shortcode() function. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-09	6.4	CVE-2026-8880
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, wrap_line (app/modules/common/common.py:181-186) and highlight_word (app/modules/common/common.py:188-192) build raw HTML by string concatenation with no escaping. The frontend (app/static/js/script.js, log-viewer paths) uses .html(data) / .append(data) to inject the response body. Anyone able to write a line into a managed HAProxy/Nginx access log (i.e. anyone who can send an HTTP request to the public LB) can land an <svg/onload= > payload that executes when a Roxy-WI admin opens the log viewer. At time of publication, there are no publicly available patches.	2026-06-10	6.1	CVE-2026-45560
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, the /smon/agent/{version,uptime,status,checks}/<server_ip> family of routes takes the URL path component verbatim into requests.get(f'http://{server_ip}:{agent_port}/...'). The path component is constrained only by Flask's default URL converter, which permits any value (including IPv4 literals like 169.254.169.254, RFC1918 ranges, and 127.0.0.1). At time of publication, there are no publicly available patches.	2026-06-10	6.5	CVE-2026-45561
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, the login flow allow-lists next URLs by rejecting strings containing https:// or http:// substrings, then constructs https://{request.host}{next_url} and the JS client redirects via window.location.replace(). The block does not consider the userinfo@host syntax. next=@evil.example/path produces https://victim.example@evil.example/path, which all modern browsers route to evil.example. At time of publication, there are no publicly available patches.	2026-06-10	6.1	CVE-2026-45566
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, get_ldap_email (app/modules/roxywi/user.py:120-157) builds the LDAP search filter via f-string concatenation. The username URL path parameter is taken verbatim - no checkAjaxInput, no LDAP escape - and inserted, a username like	2026-06-10	4.9	CVE-2026-45559

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	)(mail=)(cn=* injects additional clauses, allowing the admin to enumerate or harvest attributes outside the intended record. At time of publication, there are no publicly available patches.			
roxy-wi--roxy-wi	Roxy-WI is a web interface for managing Haproxy, Nginx, Apache and Keepalived servers. In versions 8.2.6.4 and prior, GET /history/<service>/<server_ip> re-uses the server_ip path parameter as a user-id when service == 'user', with no authorization check. Any authenticated user - even a guest in an unrelated group - can list any other user's full action audit trail (server IPs touched, configs deployed, services restarted). At time of publication, there are no publicly available patches.	2026-06-10	4.3	CVE-2026-45563
saas.group--Juicer	Juicer through 1.12.18 fails to escape remote feed API response fields before rendering them on the admin settings page. Attackers controlling the connected feed data can inject script that executes in an administrator's browser when the settings page loads.	2026-06-10	6.1	CVE-2026-53737
SAP_SE--ODP Data Replication APIs	The Remote Function Call (RFC) modules of the Operational Data Provisioning Data Replication API (ODP-RFC) are missing caller identification of permitted SAP-internal applications and are being used by customer or third-party applications in ways that are not aligned with its intended usage. Which could lead to unintended disclosure of data, but does not affect integrity, and poses minimal availability concerns for the application.	2026-06-09	6.6	CVE-2026-44754
SAP_SE--SAP Business Objects Business Intelligence Platform	SAP Business Objects Business Intelligence Platform does not sufficiently validate email sending parameters supplied by authenticated users, resulting in an email spoofing vulnerability. This vulnerability has a low impact on integrity and does not affect the confidentiality and availability of the application.	2026-06-09	4.3	CVE-2026-44755
SAP_SE--SAP Fiori (launchpad)	SAP Fiori Launchpad allows attackers to craft malicious URLs that triggers arbitrary service calls on the Fiori domain, this when opened by the user could compromise accounts by stealing user credentials. Successful exploitation requires adversaries to possess advanced knowledge of the system causing low impact on Confidentiality and Integrity. Availability of the system is no impacted.	2026-06-09	4.2	CVE-2026-24315
SAP_SE--SAP MDG (Review Match Groups Application)	SAP MDG (Review Match Groups Application) does not perform the necessary authorization checks for authenticated users. This could allow a low-privileged user to perform actions that would otherwise be restricted, resulting in escalation of privileges. This has a low impact on integrity, while confidentiality and availability are not impacted.	2026-06-09	4.3	CVE-2026-44750
SAP_SE--SAP NetWeaver AS Java (JDBC Test Servlet)	Due to a reflected cross-site scripting (XSS) vulnerability in SAP NetWeaver JAVA (JDBC Test Servlet), an unauthenticated attacker could craft a URL that embeds a malicious script. If a victim clicks this link, the injected input is processed during web page generation, resulting in the execution of malicious content in the victim's browser. This could allow the attacker to access and/or modify information related to the webclient, impacting the confidentiality and integrity of the application, with no impact to availability.	2026-06-09	6.1	CVE-2026-44746
SAP_SE--SAP S/4HANA	SAP S/4HANA(On-Premise) contains SQL injection vulnerability in a remote-enabled function module component that could be exploited by an authenticated attacker to potentially execute unauthorized database	2026-06-09	6.5	CVE-2026-44744

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	queries.This flaw exposes sensitive information to which they should not otherwise have access to. The vulnerability has a high impact on the confidentiality of the data with no impact on the integrity and availability of the application.			
SAP_SE--SAP Wily Introscope Enterprise Manager	SAP Wily Introscope Enterprise Manager allows an unauthenticated attacker to craft a specially crafted URL. Under certain conditions, when accessed by a victim, the injected script could execute in the user's browser within the context of the application. This issue has a low impact on the confidentiality and integrity of the application with no impact on availability.	2026-06-09	4.7	CVE-2026-44757
shortpixel--Enable Media Replace	The Enable Media Replace plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'location_dir' parameter in all versions up to, and including, 4.1.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-09	6.4	CVE-2026-5714
Siemens--SINEC INS	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 6). The affected application does not properly sanitize path input in the `GET /api/sftp/uploadFiles` endpoint used for directory listing. This allows path traversal through crafted input, enabling access to unintended file system locations.	2026-06-09	4.3	CVE-2026-46747
Siemens--SIPROTEC 5 6MD84 (CP300)	A vulnerability has been identified in SIPROTEC 5 6MD84 (CP300) (All versions), SIPROTEC 5 6MD85 (CP200) (All versions), SIPROTEC 5 6MD85 (CP300) (All versions), SIPROTEC 5 6MD86 (CP200) (All versions), SIPROTEC 5 6MD86 (CP300) (All versions), SIPROTEC 5 6MD89 (CP300) (All versions), SIPROTEC 5 6MU85 (CP300) (All versions), SIPROTEC 5 7KE85 (CP200) (All versions), SIPROTEC 5 7KE85 (CP300) (All versions), SIPROTEC 5 7SA82 (CP100) (All versions), SIPROTEC 5 7SA82 (CP150) (All versions), SIPROTEC 5 7SA86 (CP200) (All versions), SIPROTEC 5 7SA86 (CP300) (All versions), SIPROTEC 5 7SA87 (CP200) (All versions), SIPROTEC 5 7SA87 (CP300) (All versions), SIPROTEC 5 7SD82 (CP100) (All versions), SIPROTEC 5 7SD82 (CP150) (All versions), SIPROTEC 5 7SD86 (CP200) (All versions), SIPROTEC 5 7SD86 (CP300) (All versions), SIPROTEC 5 7SD87 (CP200) (All versions), SIPROTEC 5 7SD87 (CP300) (All versions), SIPROTEC 5 7SJ81 (CP100) (All versions), SIPROTEC 5 7SJ81 (CP150) (All versions), SIPROTEC 5 7SJ82 (CP100) (All versions), SIPROTEC 5 7SJ82 (CP150) (All versions), SIPROTEC 5 7SJ85 (CP200) (All versions), SIPROTEC 5 7SJ85 (CP300) (All versions), SIPROTEC 5 7SJ86 (CP200) (All versions), SIPROTEC 5 7SJ86 (CP300) (All versions), SIPROTEC 5 7SK82 (CP100) (All versions), SIPROTEC 5 7SK82 (CP150) (All versions), SIPROTEC 5 7SK85 (CP200) (All versions), SIPROTEC 5 7SK85 (CP300) (All versions), SIPROTEC 5 7SL82 (CP100) (All versions), SIPROTEC 5 7SL82 (CP150) (All versions), SIPROTEC 5 7SL86 (CP200) (All versions), SIPROTEC 5 7SL86 (CP300) (All versions), SIPROTEC 5 7SL87 (CP200) (All versions), SIPROTEC 5 7SL87 (CP300) (All versions), SIPROTEC 5 7SS85 (CP200) (All versions), SIPROTEC 5 7SS85 (CP300) (All versions), SIPROTEC 5 7ST85 (CP200) (All versions), SIPROTEC 5 7ST85 (CP300) (All versions), SIPROTEC 5 7ST86 (CP300) (All versions), SIPROTEC 5 7SX82 (CP150) (All versions), SIPROTEC 5 7SX85 (CP300) (All versions), SIPROTEC 5 7SY82 (CP150) (All versions), SIPROTEC 5 7UM85 (CP300) (All versions), SIPROTEC 5 7UT82 (CP100) (All versions), SIPROTEC 5 7UT82 (CP150) (All versions), SIPROTEC 5 7UT85 (CP200) (All versions), SIPROTEC 5 7UT85	2026-06-09	6.1	CVE-2025-40808

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(CP300) (All versions), SIPROTEC 5 7UT86 (CP200) (All versions), SIPROTEC 5 7UT86 (CP300) (All versions), SIPROTEC 5 7UT87 (CP200) (All versions), SIPROTEC 5 7UT87 (CP300) (All versions), SIPROTEC 5 7VE85 (CP300) (All versions), SIPROTEC 5 7VK87 (CP200) (All versions), SIPROTEC 5 7VK87 (CP300) (All versions), SIPROTEC 5 7VU85 (CP300) (All versions), SIPROTEC 5 Compact 7SX800 (CP050) (All versions). The affected application allows authenticated users to upload arbitrary files using DIGSI 5 protocol. This could allow an attacker to upload malicious configuration files, that could cause denial of service condition and potentially lead to code execution.			
signalwire-- freeswitch	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.0, FreeSWITCH includes a vulnerable function, PREFIX(prologTok()), in libs/xmlrpc-c/lib/expat/xmltok/xmltok_impl.c, which was cloned from an outdated and vulnerable version in libexpat/libexpat. The function did not receive the corresponding security patch. This issue has been patched in version 1.11.0.	2026-06-09	5.3	CVE-2026-49472
signalwire-- freeswitch	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.1, mod_verto's JSON-RPC handler bound the connection to the client-supplied sessid on the first frame, before the authentication gate. Binding inserts the connection into the global session hash and, on a key collision, drops the prior occupant of that slot - sending it a verto.punt, detaching its calls, and closing its socket. An unauthenticated network attacker who knows a target session UUID could therefore evict the legitimate client. This issue has been patched in version 1.11.1.	2026-06-09	5.3	CVE-2026-49843
signalwire-- freeswitch	FreeSWITCH is a Software Defined Telecom Stack enabling the digital transformation from proprietary telecom switches to a software implementation that runs on any commodity hardware. Prior to version 1.11.1, mod_verto's check_auth userauth branch wrote request-supplied userVariables into the connection state before comparing the supplied password. The writes are append-only and the connection is not closed on a failed compare, so values declared on bad-password attempts persisted on the same WebSocket and carried into a subsequent successful login on that connection. This issue has been patched in version 1.11.1.	2026-06-09	4.3	CVE-2026-49848
Silverpeas-- Silverpeas	Silverpeas through 6.4.6 mishandles the "Personal space" feature that is selected when no componentId is set.	2026-06-10	6.5	CVE-2026-53698
smithyqh-- sqladmin	SQLAdmin is a flexible Admin interface for SQLAlchemy models. Prior to version 0.25.1, the ajax_lookup endpoint in application.py bypasses the is_accessible() access control check that all other endpoints enforce. If a developer restricts model access by overriding is_accessible(), an authenticated user can still query that model's data through the ajax_lookup endpoint - silently bypassing the restriction. This issue has been patched in version 0.25.1.	2026-06-10	4.3	CVE-2026-46645
smub--aThemes Addons for Elementor	The aThemes Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'title_tag' Widget Setting in all versions up to, and including, 1.1.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with	2026-06-10	6.4	CVE-2026-8613

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This affects the Posts Timeline widget as well as the Posts Carousel widget across its default, Banner, and Modern skins, all of which omit the whitelist validation that is correctly applied in the Posts List widget.			
softaculous-- Page Builder: Pagelayer Drag and Drop website builder	The Page Builder: Pagelayer - Drag and Drop website builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Anchor block in versions up to, and including, 2.0.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-13	6.4	CVE-2026-3297
softaculous-- Page Builder: Pagelayer Drag and Drop website builder	The Page Builder: Pagelayer - Drag and Drop website builder plugin for WordPress is vulnerable to Incorrect Authorization in all versions up to, and including, 2.0.9. This is due to the pagelayer_save_content AJAX handler allowing users with basic post-edit capability to persist pagelayer_contact_templates metadata on posts they can edit (including pending posts), while the unauthenticated pagelayer_contact_submit endpoint later consumes that metadata by user-controlled post/form identifiers without enforcing a privileged or published-context boundary. This makes it possible for authenticated attackers, with Contributor-level access and above, to configure arbitrary contact-form mail templates that are usable through unauthenticated form submission via the contacts parameter. In typical deployments this template feature is configured via Pagelayer Pro UI; however, the vulnerable backend trust path is still present. This issue may be chained with CVE-2026-2442 to increase exploitability and attacker control over outbound email behavior.	2026-06-13	4.3	CVE-2026-2470
SolarWinds-- Observability Self-Hosted	A vulnerability in which an attacker can provide a crafted external URL that may redirect a user to an unintended website.	2026-06-09	4.8	CVE-2026-28301
solidtime-io-- solidtime	Solidtime is an open-source time-tracking app. Prior to version 0.12.2, Solidtime defines an explicit invitations:view and members:view permissions that gates the official invitations and members API. The Jetstream web team page authorizes access with only belongsToTeam() and then loads and serializes all pending invitation emails as well as members into Inertia props. Any employee who belongs to the organization can read pending invitation email addresses and members through the serialised inertia data in the team page body even though the same user is forbidden from the API. This issue has been patched in version 0.12.2.	2026-06-12	4.3	CVE-2026-47236
SourceCodester-- Barangay Resident Profiling and Information Management System	A vulnerability has been found in SourceCodester Barangay Resident Profiling and Information Management System 1.0. The impacted element is an unknown function of the file password_reset.php of the component Password Reset Handler. Such manipulation of the argument new_password with the input password123 leads to use of hard-coded password. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2026-06-08	5.3	CVE-2026-11515
SourceCodester-- CET Automated Grading System	A vulnerability has been found in SourceCodester CET Automated Grading System with AI Predictive Analytics 1.0. The impacted element is an unknown function of the file /index.php. The manipulation of the	2026-06-13	4.3	CVE-2026-12176

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
with AI Predictive Analytics	argument action leads to cross site scripting. The attack is possible to be carried out remotely. The exploit has been disclosed to the public and may be used.			
SourceCodester--Inventory System	A security flaw has been discovered in SourceCodester Inventory System 1.0. Affected by this vulnerability is an unknown functionality of the file /Product_Inventory/api/users_handler.php of the component Account Creation Handler. The manipulation of the argument ROLE results in improper authorization. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	2026-06-08	6.3	CVE-2026-11519
SourceCodester--Inventory System	A vulnerability was identified in SourceCodester Inventory System 1.0. Affected is an unknown function of the file /users.php of the component User Management Page. The manipulation of the argument fullname/username leads to cross site scripting. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	2026-06-08	4.3	CVE-2026-11518
SourceCodester--Online Examination & Learning Management System	A vulnerability has been found in SourceCodester Online Examination & Learning Management System and Syllabus-aligned Learning Management and Examination System 1.0. Affected by this issue is some unknown functionality of the file import_users.php. The manipulation of the argument raw_password with the input CICT_2026 leads to use of hard-coded password. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. This product is distributed under two entirely different names.	2026-06-08	5.3	CVE-2026-11552
Sparkle WP--MetroStore	Missing Authorization vulnerability in Sparkle WP MetroStore metrostore allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects MetroStore: from n/a through 1.3.2.	2026-06-11	4.3	CVE-2023-32959
spearman--unbounded-spsc	unbounded_spssc is an "unbounded" extension of bounded_spssc_queue. In versions 0.2.0 and prior, sender::send pointer-as-value transmute causes OOB read and fake-Arc drop under TX/RX race. At time of publication, there are no publicly available patches.	2026-06-12	5.8	CVE-2026-46690
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.2.4, 10.0.7, 9.4.12, and 9.3.13, and Splunk Cloud Platform versions below 10.3.2512.13, 10.2.2510.15, 10.1.2507.23, and 9.3.2411.132, a low-privileged user that does not hold the 'admin' or 'power' Splunk roles could craft a malicious classic dashboard that exfiltrates sensitive data to an external server when a higher-privileged user views it, bypassing the external content restriction through a Cascading Style Sheets (CSS) injection. The Trusted Domains security check does not fully validate inline style attribute values, which can allow for outbound requests to untrusted domains and credential exfiltration when a victim views a crafted dashboard.	2026-06-10	5.7	CVE-2026-20254
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.2.4, 10.0.7, 9.4.12, and 9.3.13, and Splunk Cloud Platform versions below 10.3.2512.13, 10.2.2510.15, 10.1.2507.23, and 9.3.2411.132, a low-privileged user that does not hold the "admin" or "power" Splunk roles could craft a malicious classic dashboard that exfiltrates sensitive data to an external server. The vulnerability exists because URL validation on the external content dialog is incomplete, which can allow for requests to untrusted domains when a user interacts with a crafted dashboard.	2026-06-10	5.7	CVE-2026-20255

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.2.4, 10.0.7, 9.4.12, and 9.3.13, and Splunk Cloud Platform versions below 10.3.2512.13, 10.2.2510.15, 10.1.2507.23, and 9.3.2411.132, a low-privileged user that does not hold the 'admin' or 'power' Splunk roles could cause data exfiltration through classic dashboards by redirecting a victim to an external site using a protocol-relative URL in a drill-down link. The vulnerability exists because the URL classifier in classic dashboards only recognizes 'http://' and 'https://' schemes when checking for external URLs. Protocol-relative URLs such as '//attacker.com' bypass this check entirely, and Splunk Web does not show the external-navigation warning dialog to the victim.	2026-06-10	5.7	CVE-2026-20256
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.2.4, 10.0.7, 9.4.12, and 9.3.13, and Splunk Cloud Platform versions below 10.3.2512.13, 10.2.2510.15, 10.1.2507.23, and 9.3.2411.132, a low-privileged user that does not hold the "admin" or "power" Splunk roles could craft a classic dashboard that exfiltrates sensitive data from the browser of a higher-privileged user who views it. The exfiltration is possible because classic dashboard panels do not fully validate style attribute values, which can allow for requests to reach external domains outside the configured Trusted Domains List. The vulnerability requires the attacker to phish the victim by tricking them into initiating a request within their browser. The low-privileged user should not be able to exploit the vulnerability at will.	2026-06-10	5.7	CVE-2026-20257
Splunk--Splunk Enterprise	In Splunk Enterprise versions below 10.2.4 and 10.0.7, and Splunk Cloud Platform versions below 10.4.2604.0, 10.3.2512.12, 10.2.2510.15, 10.1.2507.23, 10.0.2503.14, and 9.3.2411.131, a user who holds a Splunk role that contains the high-privilege capability 'edit_saved_search_owner' could reassign saved search ownership to users outside their authorized scope. The ownership reassignment endpoint lacks access control.	2026-06-10	5.5	CVE-2026-20259
Splunk--Splunk SOAR	In Splunk SOAR (Security Orchestration, Automation, and Response) versions below 8.5.0, an unauthenticated attacker could inject American National Standards Institute (ANSI) escape codes into SOAR application log files through specially crafted HTTP request paths, which a terminal emulator might interpret when an administrator views the logs. The injection is possible because SOAR does not strip control characters from HTTP request paths before writing them to application logs.	2026-06-10	4.3	CVE-2026-20260
Spring--Reactor Netty	In specific scenarios involving HTTP redirects from a secure to an insecure endpoint, the Reactor Netty HTTP client may leak credentials. In order for this to happen, the HTTP client must have been explicitly configured to follow redirects. Affected versions: Reactor Netty 1.0.0 through 1.0.51; 1.1.0 through 1.1.35; 1.2.0 through 1.2.17; 1.3.0 through 1.3.5.	2026-06-09	6.1	CVE-2026-41715
Spring--Spring AMQP	Correlation IDs for replies in the RabbitTemplate.sendAndReceive() with the fixed reply queue are predictable due to internal simple counter. Affected versions: Spring AMQP 4.0.0 through 4.0.3; 3.2.0 through 3.2.10; 3.1.0 through 3.1.15; 2.4.0 through 2.4.17.	2026-06-09	4.4	CVE-2026-41701
Spring--Spring AMQP	Applications that configure their broker connection via RabbitConnectionFactoryBean.setUri("amqs://...") without also calling setUseSSL(true) get TLS encryption with no certificate validation and no hostname verification. Affected versions: Spring AMQP 4.0.0 through 4.0.3; 3.2.0 through 3.2.10; 3.1.0 through 3.1.15; 2.4.0 through 2.4.17.	2026-06-09	4	CVE-2026-41714

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Spring--Spring Boot	Spring Boot's Mail auto-configuration does not enable hostname verification. Applications that set the relevant JavaMail property, such as <code>spring.mail.properties.mail.smtp.ssl.checkserveridentity=true</code> , are not affected. Affected versions: Spring Boot 4.0.0 through 4.0.6; 3.5.0 through 3.5.14; 3.4.0 through 3.4.16.	2026-06-11	5	CVE-2026-40992
Spring--Spring Boot	Spring Boot's ArtemisEmbeddedConfigurationFactory uses a fixed, static path for the embedded Artemis message broker's data directory when no explicit path is configured. A local attacker on the same host can pre-create this predictable directory or place a symlink before the application starts. Affected versions: Spring Boot 4.0.0 through 4.0.6; 3.5.0 through 3.5.14; 3.4.0 through 3.4.16; 3.3.0 through 3.3.19; 2.7.0 through 2.7.33.	2026-06-11	5.3	CVE-2026-41001
Spring--Spring Data Commons	Applications using Spring Data Commons may be vulnerable to a Denial of Service (DoS) attack leading to a StackOverflowException when parsing Sort parameters. Affected versions: Spring Data Commons 4.0.0 through 4.0.5; 3.5.0 through 3.5.11; 3.4.0 through 3.4.14; 3.3.0 through 3.3.16; 3.2.0 through 3.2.15; 3.1.0 through 3.1.14; 3.0.0 through 3.0.15; 2.7.0 through 2.7.19.	2026-06-09	5.9	CVE-2026-41711
Spring--Spring Data Commons	Spring Data Commons contains a vulnerability that can lead to a Denial of Service (DoS) condition if Spring Data Web Support is enabled in conjunction with a Controller method using <code>@ProjectedPayload</code> , when an attacker sends a specially crafted HTTP request that causes the application to allocate lots of memory. Affected versions: Spring Data Commons 4.0.0 through 4.0.5; 3.5.0 through 3.5.11; 3.4.0 through 3.4.14; 3.3.0 through 3.3.16; 3.2.0 through 3.2.15; 3.1.0 through 3.1.14; 3.0.0 through 3.0.15; 2.7.0 through 2.7.19.	2026-06-09	5.9	CVE-2026-41721
Spring--Spring Data KeyValue	A SpEL Injection vulnerability exists in the Spring Data KeyValue if unsanitized user input is passed as Sort into a repository query method that delegates evaluation to the <code>SpelPropertyComparator</code> . Affected versions: Spring Data KeyValue / Spring Data Redis 4.0.0 through 4.0.5; 3.5.0 through 3.5.11; 3.4.0 through 3.4.14; 3.3.0 through 3.3.16; 3.2.0 through 3.2.15; 3.1.0 through 3.1.14; 3.0.0 through 3.0.15; 2.7.0 through 2.7.19.	2026-06-09	6.4	CVE-2026-41719
Spring--Spring Data MongoDB	Spring Data MongoDB repository query methods annotated with <code>@Query</code> that use regex parameter binding perform insufficient validation of the bound parameter. An attacker can supply a crafted string to break out of the intended regular expression quoting. Affected versions: Spring Data MongoDB 5.0.0 through 5.0.5; 4.5.0 through 4.5.11; 4.4.0 through 4.4.14; 4.3.0 through 4.3.16; 4.2.0 through 4.2.15; 4.1.0 through 4.1.14; 4.0.0 through 4.0.15; 3.4.0 through 3.4.19.	2026-06-09	5.9	CVE-2026-41696
Spring--Spring Data Relational	Spring Data Relational does not properly escape binding values of externally-controlled input when using StringMatcher (STARTING, ENDING, or CONTAINING) in Query By Example (QBE). An attacker can supply wildcard characters to perform boolean-based blind data inference. Affected versions: Spring Data Relational/JDBC/R2DBC 4.0.0 through 4.0.5; 3.5.0 through 3.5.11; 3.4.0 through 3.4.14; 3.3.0 through 3.3.16; 3.2.0 through 3.2.15; 3.1.0 through 3.1.14; 3.0.0 through 3.0.15; 2.4.0 through 2.4.19.	2026-06-09	4.8	CVE-2026-41697

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Spring--Spring Data REST	Spring Data REST serializes the full exception cause chain into HTTP error response bodies, potentially exposing persistence-layer internals to HTTP clients. Affected versions: Spring Data REST 3.7.0 through 3.7.19; 4.3.0 through 4.3.16; 4.4.0 through 4.4.14; 4.5.0 through 4.5.11; 5.0.0 through 5.0.5.	2026-06-09	5.3	CVE-2026-41730
Spring--Spring Data REST	Spring Data REST's Querydsl integration accepts arbitrary persistent property paths as request-parameter filter keys and does not consider Jackson customizations before handing them to Querydsl. Affected versions: Spring Data REST 3.7.0 through 3.7.19; 4.3.0 through 4.3.16; 4.4.0 through 4.4.14; 4.5.0 through 4.5.11; 5.0.0 through 5.0.5.	2026-06-09	5.3	CVE-2026-41837
Spring--Spring for Apache Kafka	When an application opts into DelegatingDeserializer, a producer can grow the consumer's heap without bound by sending records with unique random spring.kafka.serialization.selector header values, eventually causing GC thrash and OutOfMemoryError. Affected versions: Spring for Apache Kafka 4.0.0 through 4.0.5; 3.3.0 through 3.3.15; 3.2.0 through 3.2.13; 2.9.0 through 2.9.13; 2.8.0 through 2.8.11.	2026-06-09	6.5	CVE-2026-41726
Spring--Spring for Apache Kafka	Spring Kafka's retry topic infrastructure did not sufficiently validate user-controlled header values before acting on them. A producer could send a record with a crafted retry_topic-attempts header to supply an out-of-range attempt count and cause the retry topic router to misidentify where the message was in the retry sequence. Affected versions: Spring for Apache Kafka 4.0.0 through 4.0.5; 3.3.0 through 3.3.15; 3.2.0 through 3.2.13; 2.9.0 through 2.9.13; 2.8.0 through 2.8.11.	2026-06-09	6.5	CVE-2026-41727
Spring--Spring Framework	Spring WebFlux applications are vulnerable to Denial of Service (DoS) attacks when processing multipart requests. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	5.9	CVE-2026-41840
Spring--Spring Framework	Spring MVC and WebFlux applications are vulnerable to Information Disclosure attacks when resolving static resources. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	5.9	CVE-2026-41841
Spring--Spring Framework	Spring MVC and WebFlux applications are vulnerable to Path Traversal attacks when resolving static resources. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	5.9	CVE-2026-41843
Spring--Spring Framework	Spring MVC applications which accept user-supplied values in the cssClass, cssErrorClass, or cssStyle attributes of JSP form tags allow arbitrary HTML/JavaScript code injection, potentially resulting in a cross-site scripting (XSS) vulnerability. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	5.9	CVE-2026-41846
Spring--Spring Framework	Applications which accept user-supplied Spring Expression Language (SpEL) expressions may be vulnerable to a Denial of Service (DoS) attack if the evaluation of a SpEL expression triggers unbounded cache growth. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	5.3	CVE-2026-41851

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Spring--Spring Framework	Spring MVC and WebFlux applications are vulnerable to Multipart request smuggling attacks. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	5.3	CVE-2026-41853
Spring--Spring Framework	IDs for WebSocket sessions in the spring-websocket module are not cryptographically unpredictable, which may be possible to exploit in combination with inadequate authorization rules. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	4.8	CVE-2026-41838
Spring--Spring Framework	A WebFlux application with a compromised subdomain (for example, compromised via cross-site scripting (XSS)) is vulnerable to an escalation attack exchanging a known session ID for that of an authenticated user. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	4.2	CVE-2026-41839
Spring--Spring Framework	A Spring MVC or Spring WebFlux application which configures a mapping for "/"**" where the view name is not explicitly specified allows an attacker to craft a link resulting in a 302 redirect to an arbitrary external host via the redirect: prefix. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	4.2	CVE-2026-41844
Spring--Spring Framework	Spring WebFlux applications may be vulnerable to a security bypass when using the Kotlin Router DSL. Affected versions: Spring Framework 5.3.0 through 5.3.48.	2026-06-09	4.8	CVE-2026-41847
Spring--Spring Framework	Due to incorrect host parsing, applications that rely on UriComponentsBuilder to parse and validate an externally provided URL string may be exposed to a server-side request forgery (SSRF) attack. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18.	2026-06-09	4.2	CVE-2026-41854
Spring--Spring REST Docs	When using spring-restdocs-webtestclient or spring-restdocs-restassured to document a remote API accessed over HTTP, an attacker who compromises the API or tricks the user into documenting a malicious API can perform an XXE injection attack when the documentation-generating tests are next executed. Affected versions: Spring REST Docs 4.0.0; 3.0.0 through 3.0.5; 2.0.0.RELEASE through 2.0.8.RELEASE.	2026-06-09	5.9	CVE-2026-40991
Spring--Spring Retry	An attacker can craft a large number of unique requests that trigger a failure, exhausting the capacity of the application-wide stateful retry cache. Once the cache is full, it permanently rejects any further updates, causing all later stateful retries and circuit breakers in the application to fail. Affected versions: Spring Retry 2.0.0 through 2.0.12; 1.3.0 through 1.3.4.	2026-06-09	5.9	CVE-2026-41710
Spring--Spring Security	Spring Security Authorization Server's authorization endpoint performs insufficient validation of the request_uri parameter. An attacker can craft a malicious authorization request containing an invalid request_uri and an arbitrary, unvalidated redirect_uri, which can lead to an Open Redirect vulnerability. Affected versions: Spring Security 7.0.0 through 7.0.5. Spring Authorization Server 1.5.0 through 1.5.7.	2026-06-09	6.1	CVE-2026-41008
Spring--Spring Security	Spring Security's CookieRequestCache and CookieServerRequestCache store the pre-authentication request URL in a browser cookie so that users can be redirected back to their intended destination after a successful	2026-06-09	6.1	CVE-2026-41706

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	login. In affected versions, the full absolute URL is stored in the cookie and is used without validation as the post-login redirect target. Affected versions: Spring Security 5.7.0 through 5.7.23; 5.8.0 through 5.8.25; 6.3.0 through 6.3.16; 6.4.0 through 6.4.16; 6.5.0 through 6.5.10; 7.0.0 through 7.0.5.			
Spring--Spring Security	SubjectDnX509PrincipalExtractor does not correctly handle certain malformed X.509 certificate CN values, which can lead to reading the wrong value for the username. In a carefully crafted certificate, this can lead to an attacker impersonating another user. Affected versions: Spring Security 5.7.0 through 5.7.24; 5.8.0 through 5.8.26; 6.3.0 through 6.3.17; 6.4.0 through 6.4.17; 6.5.0 through 6.5.10.	2026-06-09	6.8	CVE-2026-47838
Spring--Spring Web Flow	Applications that configure the WebFlowELExpressionParser are vulnerable to the use of malicious Unified EL expressions. Affected versions: Spring Web Flow 4.0.0; 3.0.0 through 3.0.1; 2.5.0 through 2.5.1.	2026-06-11	6.4	CVE-2026-40985
Spring--Spring Web Flow	Spring Web Flow's JavaScript RemotingHandler renders the body of an error response as HTML even when the response is not "text/html", which can result in a scripting attack in the user's browser if the error response from the server contains error details with input reflected from an attacker. Affected versions: Spring Web Flow 4.0.0; 3.0.0 through 3.0.1; 2.5.0 through 2.5.1.	2026-06-11	4.8	CVE-2026-40986
Spring--Spring Web Services	X509AuthenticationProvider could issue a fully authenticated X509AuthenticationToken when a presented certificate mapped to UserDetails, without applying Spring Security's standard account lifecycle checks (disabled, locked, expired, or credentials-expired accounts). Affected versions: Spring Web Services 5.0.0 through 5.0.1; 4.1.0 through 4.1.3; 4.0.0 through 4.0.18; 3.1.0 through 3.1.8.	2026-06-11	5.4	CVE-2026-40995
Spring--Spring Web Services	Several Spring WS integration paths with Spring Security could surface detailed account state (for example locked or disabled user semantics) to remote SOAP clients through exception messages or callback outcomes, instead of failing with generic authentication errors. That behavior assists remote attackers in distinguishing valid accounts from invalid ones and inferring lifecycle state. Affected versions: Spring Web Services 5.0.0 through 5.0.1; 4.1.0 through 4.1.3; 4.0.0 through 4.0.18; 3.1.0 through 3.1.8.	2026-06-11	5.3	CVE-2026-40997
Spring--Spring Web Services	Wss4jSecurityInterceptor defaulted allowRSA15KeyTransportAlgorithm to true, overriding Apache WSS4J's safer default for validation RequestData. Inbound WS-Security decryption could therefore accept RSA PKCS#1 v1.5 (rsa-1_5) encrypted key material unless operators explicitly reconfigured the flag. Affected versions: Spring Web Services 5.0.0 through 5.0.1; 4.1.0 through 4.1.3; 4.0.0 through 4.0.18; 3.1.0 through 3.1.8.	2026-06-11	4.8	CVE-2026-40996
stefanbohacek--fediverse-embeds-wordpress-plugin	Fediverse Embeds embeds fediverse posts on WordPress sites. Prior to version 1.5.9, Fediverse Embeds registered the unauthenticated AJAX action wp_ajax_nopriv_ftf_get_site_info (includes/Site_Info.php) that verified a nonce ftf-fediverse-embeds-nonce and then called file_get_html(\$site_url) on the attacker-supplied URL. The same nonce was enqueued onto every public page containing a fediverse embed (via includes/Enqueue_Assets.php lines 41-46 + includes/Helpers.php lines 64-83), so the nonce gate was not an authentication boundary; any visitor of a	2026-06-11	5.3	CVE-2026-46698

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	public post with an embed could grab it and reuse it. This issue has been patched in version 1.5.9.			
steipete--CodexBar	CodexBar before 0.33.0 contains a credential forwarding vulnerability that allows network-adjacent attackers to intercept sensitive credentials by issuing cross-origin or HTTP-downgrade redirects to the shared ProviderHTTPClient transport. Attackers can redirect credentialed provider requests carrying browser cookies, bearer tokens, or API keys to an unintended host, port, or plaintext HTTP destination to capture those credentials.	2026-06-11	5.3	CVE-2026-49949
steipete--summarize	Summarize before 0.17.0 contains a resource exhaustion vulnerability that allows remote attackers to cause disk exhaustion by serving media responses that bypass the enforced size limit through missing or misreported Content-Length headers, chunked transfer encoding, or failed HEAD requests. Attackers who control a podcast feed or media URL can stream an unbounded response to local storage via the temp-file download path, exhausting disk or system resources on the host running the CLI.	2026-06-11	4.3	CVE-2026-53781
subzeroid--aiograpi	aiograpi is an asynchronous Instagram API for Python. aiograpi versions before 0.9.10 accepted server-supplied signup challenge paths and used them to build request URLs before validating that the paths were relative Instagram API paths. If an attacker can influence a challenge response, for example through a local network, DNS, or proxy compromise, challenge handling requests could be sent outside the intended Instagram host with the client's existing session headers. Version 0.9.10 validates challenge paths before building URLs, solving captcha challenges, or submitting phone/SMS challenge forms.	2026-06-11	6.5	CVE-2026-47157
Systerel--S2OPC	Check for certificate revocation only considers the first matching CRL and ignores other valid CRLs of the same CA in the CycloneCrypto cryptographic wrapper of S2OPC library. It might allow connection between an OPC UA client and server using a revoked certificate.	2026-06-09	5.6	CVE-2026-6899
techjewel--WP GDPR Cookie Consent	The WP GDPR Cookie Consent plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ninja_gdpr_ajax_actions' AJAX action in versions up to, and including, 1.0.0. This is due to missing capability and nonce checks on the handleAjaxCalls() function, combined with insufficient input sanitization on the gdprConfig values and missing output escaping in the generateCSS() function which echoes stored configuration values directly into a <style> block rendered on wp_head. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-09	6.4	CVE-2026-8977
TemplateHouse--Soledad	Missing Authorization vulnerability in TemplateHouse Soledad allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects Soledad: from n/a through 8.2.5.	2026-06-11	5.4	CVE-2022-42479
Tenda--AC15	A weakness has been identified in Tenda AC15 15.03.05.19. The impacted element is an unknown function of the file /etc_ro/smb.conf of the component Samba. Executing a manipulation can lead to weak password requirements. The attack is only possible within the local network. A high complexity level is associated with this attack. The exploitability is	2026-06-08	5	CVE-2026-11493

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	regarded as difficult. The exploit has been made available to the public and could be used for attacks.			
ThemeHunk-- Contact Form & Lead Form Elementor Builder	Missing Authorization vulnerability in ThemeHunk Contact Form & Lead Form Elementor Builder allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Contact Form & Lead Form Elementor Builder: from n/a through 1.8.4.	2026-06-11	5.4	CVE-2023-25969
tierrainnovation-- AJAX Report Comments	The AJAX Report Comments plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.4. This is due to missing or incorrect nonce validation on the rc_options_page function. This makes it possible for unauthenticated attackers to modify plugin settings including link text and markup, success/failure/already-reported messages, comment threshold, cookie duration, reporter-comment toggle, and notification email address, subject, and message body via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-09	4.3	CVE-2026-8902
tigroumeow-- Meow Gallery	The Meow Gallery plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the REST API endpoint /wp-json/meow-gallery/v1/save_shortcode in all versions up to, and including, 5.4.4 This makes it possible for authenticated attackers, with Author-level access and above, to arbitrarily create or overwrite existing gallery shortcode records by supplying a user-controlled id value. The endpoint performs database update operations without verifying that the requesting user is authorized to modify the referenced gallery record or create their own.	2026-06-13	4.3	CVE-2026-1291
tmux--tmux	A security vulnerability has been detected in tmux up to 3.6a. Affected is the function image_free of the file image.c. Such manipulation leads to use after free. Local access is required to approach this attack. This attack is characterized by high complexity. The exploitability is told to be difficult. The exploit has been disclosed publicly and may be used. Upgrading to version 3.7-rc is able to address this issue. The name of the patch is fc6d94a9f8a593bd8b7031650802084385d4ee03. The affected component should be upgraded.	2026-06-09	4.5	CVE-2026-11623
TOTOLINK-- AC1200 T8	A security vulnerability has been detected in TOTOLINK AC1200 T8 4.1.5cu.8611. This affects an unknown function of the file /etc/vsftpd.conf of the component vsftpd. The manipulation leads to least privilege violation. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used.	2026-06-08	4.3	CVE-2026-11494
TOTOLINK-- CP450	A vulnerability was determined in TOTOLINK CP450 4.1.0cu.747. This vulnerability affects unknown code of the file /etc/vsftpd.conf of the component vsftpd. This manipulation causes least privilege violation. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2026-06-08	4.3	CVE-2026-11554
TOTOLINK-- EX200	A security flaw has been discovered in TOTOLINK EX200 4.0.3c.7646. This affects an unknown function of the file /etc/vsftpd.conf of the component vsftpd. The manipulation results in least privilege violation. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks.	2026-06-09	5.3	CVE-2026-11620

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
umbraco-- Umbraco-CMS	Umbraco is an ASP.NET CMS. Prior to versions 13.14.0 and 17.4.0, some of the Surface Controllers in the CMS provide to support member related operations fail to validate redirect URLs, making Razor templates that derive 'RedirectUrl' from user-controlled query parameters vulnerable to malicious redirect attacks. This issue has been patched in versions 13.14.0 and 17.4.0.	2026-06-10	5.4	CVE-2026-46616
umbraco-- Umbraco-CMS	Umbraco is an ASP.NET CMS. From version 14.0.0 to before version 17.4.0, authenticated users are able to inject HTML into an input field, which is rendered in the confirmation dialog without proper output encoding. This issue has been patched in version 17.4.0.	2026-06-10	4.6	CVE-2026-46609
UTT--HiPER 2610G	A vulnerability was found in UTT HiPER 2610G up to 3.0.0-171107. This affects the function strcpy of the file /goform/formNatStaticMap. Performing a manipulation of the argument NatBinds results in buffer overflow. The exploit has been made public and could be used.	2026-06-08	5.5	CVE-2026-11516
wealcode-- Animation Addons for Elementor GSAP Motion Elementor Addons & Website Templates	The Animation Addons for Elementor - GSAP Powered Elementor Addons & Website Templates plugin for WordPress is vulnerable to DOM-Based Stored Cross-Site Scripting via the multiple parameters in all versions up to, and including, 2.6.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-10	6.4	CVE-2025-8444
weaverlancegma ilcom--jQuery Hover Footnotes	The jQuery Hover Footnotes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Footnote Qualifier ('{{...}}' Syntax) in all versions up to, and including, 1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The attribute-breakout payload (e.g., a double-quote followed by an event handler) contains no angle brackets and therefore bypasses WordPress core's wp_kses_post() filtering, which only strips disallowed HTML tags rather than sanitizing attribute contexts.	2026-06-09	6.4	CVE-2026-10738
weaverlancegma ilcom--jQuery Hover Footnotes	The jQuery Hover Footnotes plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.4. This is due to missing or incorrect nonce validation on the jqFootnotes_options_subpanel function. This makes it possible for unauthenticated attackers to update the plugin's settings with arbitrary values that, because option values such as jqfoot_anchor_open, jqfoot_anchor_close, and jqfoot_title are echoed unescaped into frontend page content, can be chained into persistent Cross-Site Scripting affecting all site visitors via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. Successful exploitation of the CSRF vulnerability can be chained into stored Cross-Site Scripting, as the overwritten option values are persisted via update_option() without sanitization and rendered unescaped on the frontend.	2026-06-09	4.3	CVE-2026-10553
Weaviate-- Weaviate	A vulnerability was identified in Weaviate up to 1.37.7. This vulnerability affects the function validateConfig of the file	2026-06-08	5	CVE-2026-11500

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	usecases/auth/authentication/apikey/client.go of the component Static API Key Handler. The manipulation of the argument StaticApiKey leads to authorization bypass. It is possible to initiate the attack remotely. The complexity of an attack is rather high. It is stated that the exploitability is difficult. The exploit is publicly available and might be used. Upgrading to version 1.38.0-rc.0 is able to resolve this issue. The identifier of the patch is 40f2cc32279f0f8a51016c3c6870a2c0c808e6c0. You should upgrade the affected component.			
WeblateOrg--weblate	Weblate is a web based localization tool. From version 5.15 to before version 2026.6, Weblate's VCS_RESTRICT_PRIVATE did not properly account for some transitional IPv6 ranges, multicast addresses, or some semi-private IPv4 ranges, which allowed some addresses to bypass private range restrictions. This issue has been patched in version 2026.6.	2026-06-10	5.9	CVE-2026-50127
WeblateOrg--weblate	Weblate is a web based localization tool. Prior to version 2026.5, Weblate's live search preview renders unit source and context as HTML without escaping. Any contributor whose content reaches those fields stores HTML and CSS that runs inside the authenticated editor of every user who runs a matching search. This issue has been patched in version 2026.5.	2026-06-10	4.6	CVE-2026-45106
websoudan--MW WP Form	The MW WP Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'memo' parameter in all versions up to, and including, 5.1.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Because the memo value is stored via update_post_meta() rather than wp_insert_post(), WordPress's built-inkses and unfiltered_html protections do not apply, allowing attackers to break out of the textarea element via injected closing tags regardless of role-based content filtering.	2026-06-10	4.4	CVE-2026-8853
wedevs--User Frontend: AI Powered Frontend Posting, User Directory, Profile, Membership & User Registration	The User Frontend: AI Powered Frontend Posting, User Directory, Profile, Membership & User Registration plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the user_subscription_cancel() function in all versions up to, and including, 4.3.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to cancel any user's subscription pack, including administrators.	2026-06-09	4.3	CVE-2026-4058
weDevs--WooCommerce Conversion Tracking	Cross-Site request forgery (CSRF) vulnerability in weDevs WooCommerce Conversion Tracking allows Cross Site Request Forgery. This issue affects WooCommerce Conversion Tracking: from n/a through 2.0.10.	2026-06-11	4.3	CVE-2022-47150
WP24--WP24 Domain Check	WordPress Plugin WP24 Domain Check 1.6.2 contains a stored cross-site scripting vulnerability that allows authenticated attackers to inject malicious scripts by submitting crafted input to the fieldNameDomain parameter. Attackers can inject JavaScript payloads through the plugin settings form at options.php that execute in the browsers of administrators viewing the settings page.	2026-06-08	6.4	CVE-2021-47984

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wpmessiah--Prime Elementor Addons Lightweight Elementor Widgets for Faster Pages	The Prime Elementor Addons - Lightweight Elementor Widgets for Faster Pages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Widget HTML Tag Settings in all versions up to, and including, 1.3.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The exploit succeeds even for users without the unfiltered_html capability because the payload (e.g., 'img src=x onerror=alert(document.domain)') contains no HTML angle brackets and therefore passes through Elementor's wpkses_post() filter unchanged at save time.	2026-06-09	6.4	CVE-2026-8677
wpzoom--Recipe Card Blocks Lite	The Recipe Card Blocks Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the recipe block's 'summary' and 'notes' attributes in all versions up to, and including, 3.4.13. This is due to the 'WPZOOM_Helpers::deserialize_block_attributes' method converting unicode-encoded sequences back into HTML characters after sanitization has already been applied. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that execute whenever a user accesses the published post or the print view of an injected recipe.	2026-06-08	6.4	CVE-2026-3011
yamcs--yamcs	Yamcs is a mission control framework. Prior to versions 5.13.0 and 5.12.7, an LDAP injection vulnerability exists in 'org.yamcs.security.LdapAuthModule' when constructing search filters. The username parameter is inserted directly into the LDAP filter without proper RFC 4515 escaping. Versions 5.13.0 and 5.12.7 patch the issue.	2026-06-10	4.3	CVE-2026-42568
YITH--YITH WooCommerce Product Slider Carousel	Cross-Site request forgery (CSRF) vulnerability in YITH YITH WooCommerce Product Slider Carousel allows Cross Site Request Forgery. This issue affects YITH WooCommerce Product Slider Carousel: from n/a through 1.16.0.	2026-06-11	4.6	CVE-2022-44630
yoanbernabeu--grepai	A vulnerability has been found in yoanbernabeu grepai 0.35.0. This issue affects some unknown processing of the file indexer/chunker.go of the component Qdrant Backend. Such manipulation leads to use of weak hash. The attack may be performed from remote. Attacks of this nature are highly complex. The exploitability is assessed as difficult. The exploit has been disclosed to the public and may be used. The pull request to fix this issue awaits acceptance.	2026-06-08	4.2	CVE-2026-11479
Yoast--Yoast Duplicate Post	Yoast Duplicate Post through 4.6 inserts an unescaped post title and permalink into the Classic Editor scheduled republish notice. Attackers can schedule a republish copy with a crafted title to execute script when an administrator views the resulting notice.	2026-06-10	5.4	CVE-2026-53740
Yoast--Yoast Duplicate Post	Yoast Duplicate Post through 4.6 contains a cross-site request forgery vulnerability in the duplicate_post_dismiss_notice handler, which verifies no nonce or capability. Attackers can trick any authenticated user into sending a request that sets the duplicate_post_show_notice site option, suppressing admin notices network-wide.	2026-06-10	4.3	CVE-2026-53739
yuluma--FastPicker, an order picker and order	The FastPicker, an order picker and order management system (oms) for WooCommerce on steroids plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.2. This is due to missing or incorrect nonce validation on the settingsPage function. This	2026-06-09	4.3	CVE-2026-8904

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
management system (oms) for WooCommerce on steroids	makes it possible for unauthenticated attackers to modify the plugin's settings, including toggling the webhook integration and changing the FastPicker and KDZ API URLs via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.			
10web--Form Maker by 10Web Mobile-Friendly Drag & Drop Contact Form Builder	The Form Maker by 10Web - Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to generic SQL Injection via the 'groupids' parameter in all versions up to, and including, 1.15.43 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-06-18	4.9	CVE-2026-11776
10web--Form Maker by 10Web Mobile-Friendly Drag & Drop Contact Form Builder	The Form Maker by 10Web - Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to generic SQL Injection via the 'name' parameter in all versions up to, and including, 1.15.43 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-06-18	4.9	CVE-2026-11777
2download--2Download Connector for 2DL Hosted Checkout	The 2Download Connector for 2DL Hosted Checkout plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 0.1.5. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to view arbitrary customers' subscription data including subscription status, product names, order IDs, purchase dates, and expiry dates.	2026-06-19	5.3	CVE-2026-6798
abtest--Abtest	WordPress Plugin Abtest contains a local file inclusion vulnerability that allows unauthenticated attackers to include arbitrary files by manipulating the action parameter. Attackers can send GET requests to abtest_admin.php with malicious action values to include files from the admin directory and execute arbitrary code.	2026-06-15	6.2	CVE-2016-20082
AcademySoftwareFoundation--openexr	OpenEXR is the reference implementation and specification for the EXR image format, widely used in the motion picture industry. In versions 3.4.0 through 3.4.11, an integer overflow in ht_undo_impl() in src/lib/OpenEXRCore/internal_ht.cpp leads to a heap-buffer overflow when decoding a crafted HTJ2K-compressed EXR file. decode->channels[i].width (int32_t) is multiplied by bytes_per_element in 32-bit signed arithmetic. With large widths (e.g., >= 536870912 for FLOAT data), this overflows, producing a corrupted offset that is later used for pointer arithmetic and can cause a heap out-of-bounds write. The same unchecked multiplication pattern appears in two other HTJ2K paths (bytes-per-line accumulation and pixel-line pointer advancement). As with related CVE-2026-34378 through CVE-2026-34589 fixes in other codecs, validating only after the multiplication is too late because the value may already be overflowed. This issue has been fixed in version 3.4.12.	2026-06-18	6.1	CVE-2026-44663
activepieces--activepieces	A vulnerability was detected in activepieces up to 0.83.0. This vulnerability affects the function handleUrlFile in the library packages/server/engine/src/lib/variables/processors/file.ts of the	2026-06-21	6.3	CVE-2026-12813

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	component File URL Handler. The manipulation results in server-side request forgery. The attack can be executed remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.			
adamsilverstein-- User Admin Simplifier	The User Admin Simplifier plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.0.0. This is due to missing or incorrect nonce validation on the useradminsimplifier_options_page function. This makes it possible for unauthenticated attackers to reset and permanently delete any user's stored menu and admin-bar configuration via a forged request that triggers uas_save_admin_options() and overwrites the useradminsimplifier_options database entry via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-19	4.3	CVE-2026-11775
addonspress-- Advanced Import	The Advanced Import plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 1.4.6. This is due to the plugin using wp_remote_get() to fetch a user-supplied URL without validating that the URL does not point to internal or private network resources in the demo_download_and_unzip() function. The 'demo_file' parameter from \$_POST is passed through sanitize_text_field() (which only handles XSS-related sanitization) and then directly into wp_remote_get() when 'demo_file_type' is set to 'url'. Notably, the plugin uses wp_safe_remote_get() in other locations (theme template libraries) which would provide SSRF protection, but fails to use it in this critical AJAX handler. This makes it possible for authenticated attackers, with Author-level access and above (upload_files capability), to make web requests to arbitrary locations originating from the web application, which can be used to query and view data from internal services, including cloud instance metadata endpoints.	2026-06-19	6.4	CVE-2026-4328
Adobe--DNG SDK	DNG SDK versions 1.7.1 2536 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-16	5.5	CVE-2026-47927
Adobe--DNG SDK	DNG SDK versions 1.7.1 2536 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-16	5.5	CVE-2026-47934
Adobe--DNG SDK	DNG SDK versions 1.7.1 2536 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-16	5.5	CVE-2026-47963
Ahmad--JS Help Desk	Unauthenticated Broken Access Control in JS Help Desk <= 3.0.9 versions.	2026-06-15	6.5	CVE-2026-48887
Ahmad--WP Job Portal	Subscriber Cross Site Scripting (XSS) in WP Job Portal <= 2.5.2 versions.	2026-06-15	6.5	CVE-2026-48880

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
algolplus--Advanced Order Export For WooCommerce	The Advanced Order Export For WooCommerce plugin for WordPress is vulnerable to generic SQL Injection via the 'sort_direction' parameter in all versions up to, and including, 4.0.10 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with shop manager-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The endpoint requires a valid woe_nonce and Shop Manager-level capabilities (view_woocommerce_reports or export_woocommerce_orders), and wp_magic_quotes protection is stripped via stripslashes_deep() before processing, allowing quote and backslash characters to survive intact into the SQL context.	2026-06-18	4.9	CVE-2026-11360
ali2woo--AliNext	Missing Authorization vulnerability in ali2woo AliNext allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects AliNext: from n/a through 3.3.5.	2026-06-17	6.5	CVE-2024-37210
Amit Mittal--Shipment Tracker for Woocommerce	Subscriber Cross Site Scripting (XSS) in Shipment Tracker for Woocommerce <= 1.5.3.2 versions.	2026-06-15	6.5	CVE-2026-39540
Andy Moyle--Emergency Password Reset	Cross-Site request forgery (CSRF) vulnerability in Andy Moyle Emergency Password Reset allows Cross Site Request Forgery. This issue affects Emergency Password Reset: from n/a through 8.0.	2026-06-17	4.3	CVE-2024-35648
Apollo Pharmacy--Blood Glucose Monitoring System (Model No. APG-01 BT)	An attacker within BLE communication range can passively intercept wireless traffic and obtain sensitive health-related information, including glucose measurement values.	2026-06-18	6.5	CVE-2026-50034
Apollo Pharmacy--Blood Glucose Monitoring System (Model No. APG-01 BT)	An attacker within BLE communication range can monopolize the device's only available BLE connection slot, preventing legitimate users or applications from establishing a connection.	2026-06-18	6.5	CVE-2026-52866
artbees--JupiterX Core	Subscriber Cross Site Scripting (XSS) in JupiterX Core <= 4.14.1 versions.	2026-06-15	6.5	CVE-2026-39491
authlib--joserfc	joserfc is a Python library that provides an implementation of several JSON Object Signing and Encryption (JOSE) standards. In versions 1.3.4 through 1.6.5, joserfc accepts oversized RFC7797 b64=false JWS payloads without applying JWSRegistry.max_payload_length, which can lead to resource exhaustion. The normal JWS compact and flattened JSON paths reject payloads above the configured payload-size limit with ExceededSizeError. The RFC7797 unencoded payload paths do not make the same check. A valid b64=false compact or flattened JSON JWS can therefore deserialize successfully with a payload larger than JWSRegistry.max_payload_length. Applications that accept lower-trust JWS values and rely on joserfc to reject oversized token content during verification have a moderate availability risk. This issue has been fixed in version 1.6.7.	2026-06-17	5.3	CVE-2026-48990

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Autodesk--Revit	A maliciously crafted RFA file, when converted to FormIt via "Convert RFA to FormIt" in Autodesk Revit, can force a NULL Pointer Dereference vulnerability. Successful exploitation may cause the application to crash, leading to a denial-of-service condition.	2026-06-17	5.5	CVE-2026-1288
AVideo--AVideo	AVideo through version 27.0 contains a server-side request forgery vulnerability in plugin/Live/test.php that allows authenticated administrators to read arbitrary URLs via the statsURL parameter, which lacks isSSRFSafeURL() validation and accepts requests to private IP ranges and cloud metadata endpoints. Attackers can exploit this by crafting requests to internal services, cloud metadata endpoints like 169.254.169.254, and localhost to retrieve sensitive information including IAM credentials, internal service responses, and network configuration details.	2026-06-20	6.8	CVE-2026-56342
AVideo--AVideo	AVideo through version 25.0 contains an authentication bypass vulnerability in the decryptMessage.json.php endpoint that allows unauthenticated users to decrypt PGP messages. Remote attackers can submit private keys, ciphertext, and passphrases to perform server-side decryption without credentials, exposing key material to logs and enabling resource exhaustion attacks.	2026-06-20	6.5	CVE-2026-56346
Avirtum--iPages Flipbook	Missing Authorization vulnerability in Avirtum iPages Flipbook allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects iPages Flipbook: from n/a through 1.5.1.	2026-06-17	5.3	CVE-2024-33909
Awesomemotive--Envira Photo Gallery	Unauthenticated Broken Access Control in Envira Photo Gallery <= 1.12.5 versions.	2026-06-16	6.5	CVE-2026-54190
AWS--Kiro IDE	Incorrect default permissions in Kiro IDE on macOS and Linux before version 0.11.133 could expose the authentication token cache file to other local users or processes via world-readable permissions (0644) instead of owner-restricted permissions (0600). To remediate this issue, users should upgrade to Kiro IDE version 0.11.133 or later. After upgrading and restarting the application, the cache file permissions are automatically updated on the next token refresh. Users operating in a multi-user environment can invalidate existing tokens by reauthenticating.	2026-06-15	5.5	CVE-2026-11931
BerriAI--litellm	A security flaw has been discovered in BerriAI litellm up to 1.82.2. This impacts the function authenticate_user of the file litellm/proxy/auth/login_utils.py of the component PROXY_ADMIN database API Key Generator. Performing a manipulation results in session expiration. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure.	2026-06-21	6.3	CVE-2026-12772
BerriAI--litellm	A security vulnerability has been detected in BerriAI litellm up to 1.82.2. Affected by this vulnerability is the function _execute_with_mcp_client of the file litellm/proxy/_experimental/mcp_server/rest_endpoints.py of the component MCP Server Connection Testing. The manipulation leads to server-side request forgery. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure.	2026-06-21	6.3	CVE-2026-12774

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
BerriAI--litellm	A vulnerability was identified in BerriAI litellm up to 1.82.2. This impacts the function <code>get_redirect_response_from_openid</code> of the file <code>litellm/proxy/management_endpoints/ui_sso.py</code> of the component SSO Authentication Flow. The manipulation leads to session expiration. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure.	2026-06-21	6.3	CVE-2026-12796
BerriAI--litellm	A security flaw has been discovered in BerriAI litellm up to 1.82.5. Affected is the function <code>async_pre_call_hook</code> of the file <code>enterprise/enterprise_hooks/banned_keywords.py</code> of the component Completions Interface. The manipulation of the argument <code>prompt</code> results in incorrect authorization. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure.	2026-06-21	6.3	CVE-2026-12797
BerriAI--litellm	A weakness has been identified in BerriAI litellm up to 1.82.2. Affected by this vulnerability is the function <code>load_openapi_spec_async</code> of the file <code>litellm/proxy/_experimental/mcp_server/openapi_to_mcp_generator.py</code> of the component MCP OpenAPI Spec Loader. This manipulation of the argument <code>spec_path</code> causes server-side request forgery. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure.	2026-06-21	6.3	CVE-2026-12798
BerriAI--litellm	A vulnerability was determined in BerriAI litellm up to 1.63.1. The impacted element is an unknown function of the file <code>litellm/proxy/management_endpoints/key_management_endpoints.py</code> of the component Admin Key Handler. This manipulation causes improper authorization. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. Patch name: 23781. It is recommended to apply a patch to fix this issue. The vendor was contacted early about this disclosure.	2026-06-21	5.4	CVE-2026-12770
BerriAI--litellm	A vulnerability was identified in BerriAI litellm up to 1.82.2. This affects an unknown function of the file <code>litellm/proxy/auth/user_api_key_auth.py</code> of the component M2M JWT Handler. Such manipulation leads to improper authorization. The attack can be launched remotely. A high complexity level is associated with this attack. The exploitability is reported as difficult. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure.	2026-06-21	5	CVE-2026-12771
BerriAI--litellm	A security vulnerability has been detected in BerriAI litellm up to 1.82.2. Affected by this issue is the function <code>ui_view_users</code> of the file <code>litellm/proxy/management_endpoints/internal_user_endpoints.py</code> of the component Incomplete Fix CVE-2025-0628. Such manipulation leads to improper authorization. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure.	2026-06-21	4.3	CVE-2026-12799
Bitnami--bitnami/mariadb-galera	Bitnami MariaDB Galera container images and Helm chart are affected by a hardcoded default credential vulnerability in the Galera replication health-check user. The <code>MARIADB_REPLICATION_USER</code> and <code>MARIADB_REPLICATION_PASSWORD</code> environment variables defaulted to <code>monitor</code> and <code>monitor</code> respectively. This user is granted <code>REPLICATION</code>	2026-06-18	5.3	CVE-2026-47847

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CLIENT privileges from any host ('%'). The Bitnami Helm chart for MariaDB Galera did not expose parameters to configure this user's credentials, resulting in all chart deployments using this publicly known credential by default. Affected versions - Container image: 10.6.x prior to 10.6.27-photon-5-r0; 10.11.x prior to 10.11.17-photon-5-r1; 11.4.x prior to 11.4.12-photon-5-r0; 11.8.x prior to 11.8.7-photon-5-r1; 12.3.x prior to 12.3.2-photon-5-r0 / 12.3.2-debian-12-r0. Helm chart: prior to 18.3.0.			
bitpressadmin-- Bit integrations Form Integration, Webhook, Spreadsheets, CRM, LMS & Email Automation	The Bit integrations - Form Integration, Webhook, Spreadsheets, CRM, LMS & Email Automation plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.8.7 via the upload_attachment. This makes it possible for unauthenticated attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. Exploitation requires a form integration to be configured with a field mapped to a WooCommerce product image, product gallery, downloadable files, or Google Contacts attachment field, which is a default use case for these integrations.	2026-06-19	6.5	CVE-2026-11989
Black Lantern Security--BBOT	The postman_download module uses the workspace name field from the Postman API to construct the local directory path without sanitization. If a malicious workspace has a name containing path traversal characters, pathlib resolves the path outside the intended output directory, allowing an attacker to write arbitrary files to the user's system.	2026-06-17	6.5	CVE-2026-12568
Black Lantern Security--BBOT	The unarchive internal module's archive extraction commands perform no code-level validation on extracted file paths, relying entirely on the behavior of external tools (e.g. GNU tar) which varies by platform. While CVE-2025-10284 addressed git-specific RCE vectors, the underlying archive extraction path traversal was never fixed. On systems with GNU tar < 1.34 (Ubuntu 20.04, Debian Buster, CentOS 7, many Docker base images), a malicious archive can write files outside the intended extraction directory.	2026-06-17	5.3	CVE-2026-12565
blubrry-- PowerPress Podcasting plugin by Blubrry	The PowerPress Podcasting plugin by Blubrry plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'embed' Episode Meta Field in all versions up to, and including, 11.16.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The embed value is stored via update_post_meta() rather than through WordPress core's post content pipeline, meaning kses-on-save filtering is never applied - even for Author-role users who would otherwise lack unfiltered_html - making this path unprotected by WordPress's standard role-based XSS mitigations.	2026-06-18	6.4	CVE-2026-12098
BoldGrid--W3 Total Cache	Author Broken Access Control in W3 Total Cache <= 2.9.1 versions.	2026-06-17	4.7	CVE-2026-39595
Booking Activities Team-- Booking Activities	Unauthenticated Broken Access Control in Booking Activities <= 1.16.48.1 versions.	2026-06-15	6.5	CVE-2026-39525

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Bootstrapped Ventures--Visual Link Preview	Subscriber Sensitive Data Exposure in Visual Link Preview <= 2.4.1 versions.	2026-06-15	6.5	CVE-2026-48878
bplugins--Services Section Block Showcase Service Details in Grid or Columns	The Services Section Block - Showcase Service Details in Grid or Columns plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'link' Block Attribute in all versions up to, and including, 1.4.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The payload persists inside HTML comments in post_content, bypassing wp_kses_post sanitization at save time, and executes via both the primary service link anchor and a secondary title-wrapped anchor when the linkIn option is set to 'title'.	2026-06-18	6.4	CVE-2026-11402
Brandfolder--Brandfolder	WordPress Brandfolder plugin version 3.0 and earlier contains a local file inclusion vulnerability in callback.php that allows unauthenticated attackers to include arbitrary files by manipulating the wp_abspath parameter. Attackers can supply path traversal sequences or remote URLs through the wp_abspath parameter to read sensitive files like wp-config.php or execute remote code.	2026-06-15	6.2	CVE-2016-20080
Bricks--Bricks Builder	Subscriber Broken Access Control in Bricks Builder <= 2.1.4 versions.	2026-06-17	4.3	CVE-2026-40723
Bricksable--Bricksable for Bricks Builder	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bricksable for Bricks Builder allows Stored XSS. This issue affects Bricksable for Bricks Builder: from n/a through 1.6.83.	2026-06-18	5.9	CVE-2026-56009
bunny.net--bunny.net	Subscriber Broken Access Control in bunny.net <= 2.3.6 versions.	2026-06-15	6.3	CVE-2025-68049
Canon Inc.--EOS Network Setting Tool for Windows	Improper validation of SSH host keys in Canon EOS Network Setting Tool Version 1.5.0 or earlier	2026-06-15	6.5	CVE-2026-9258
Canon Inc.--EOS Network Setting Tool for Windows	Improper validation of server certificates in Canon EOS Network Setting Tool Version 1.5.0 or earlier	2026-06-15	6.5	CVE-2026-9259
Canon Inc.--EOS Network Setting Tool for Windows	Use of hard-coded cryptographic keys in Canon EOS Network Setting Tool Version 1.5.0 or earlier	2026-06-15	6.2	CVE-2026-9260
Canon Inc.--EOS Network Setting Tool for Windows	Use of weak SSH cryptographic algorithms in Canon EOS Network Setting Tool Version 1.5.0 or earlier	2026-06-15	6.8	CVE-2026-9261
Canon Inc.--EOS Network Setting Tool for Windows	Use of a non-secure protocol as the default FTP configuration in Canon EOS Network Setting Tool Version 1.5.0 or earlier	2026-06-15	6.5	CVE-2026-9262

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Cap-go--capgo	Cap-go capgo before 12.128.2 contains an authorization bypass in several Supabase PostgREST RPC functions (get_app_metrics, get_global_metrics, get_total_metrics) that are granted to the anon role without enforcing org membership or permission checks. An unauthenticated attacker using only the public Supabase API key (sb_publishable_*) can query arbitrary org_id values to disclose cross-tenant usage telemetry (MAU, bandwidth, installs, gets), enumerate app IDs for a target org, and determine org existence via an oracle (valid org returns metrics, invalid returns []).	2026-06-20	5.3	CVE-2026-56235
Cap-go--capgo	Cap-go before 12.128.2 contains an information disclosure vulnerability in the OPTIONS /build/upload/:jobId/* endpoint that allows unauthenticated attackers to enumerate valid builder job IDs through observable response discrepancies. Attackers can probe the endpoint without authentication to distinguish valid job IDs from invalid ones and generate sustained unauthenticated traffic for resource consumption.	2026-06-21	5.3	CVE-2026-56316
Cap-go--capgo	Capgo before 12.128.2 contains a flaw in the Enforce Password Policy feature: after a Super Admin enables the policy and successfully changes their password to a compliant one, the backend does not update the password-compliance state. As a result, the backend continues to treat the account as non-compliant and repeatedly forces password-reset prompts, permanently locking the Super Admin out of organization access (organization lockout / denial of service) despite valid authentication.	2026-06-19	4.9	CVE-2026-56080
Cap-go--capgo	Cap-go before 12.128.12 contains a broken cursor pagination vulnerability in the /private/devices endpoint on the Cloudflare/workerd path that allows authenticated attackers to cause duplicate-page loops and make later rows unreachable. Attackers with app.read_devices access can exploit non-advancing cursor filters to trigger infinite pagination loops, prevent dataset traversal, and cause repeated processing in device-management workflows.	2026-06-20	4.3	CVE-2026-56307
capacitor-native-biometric--capacitor-native-biometric	capacitor-native-biometric before 12.128.2 contains an authentication bypass vulnerability where the onAuthenticationSucceeded() method fails to validate CryptoObject parameters. Attackers can hook the onAuthenticationSucceeded() function using dynamic instrumentation to bypass biometric authentication without valid credentials.	2026-06-20	4.8	CVE-2026-56294
Capgo--Capgo	Capgo before 12.128.2 contains a cross-tenant authorization bypass vulnerability in PostgREST endpoints that allows org-scoped read API keys to access other tenants' webhook secrets and delivery logs. Attackers can query the webhooks and webhook_deliveries endpoints to exfiltrate HMAC signing secrets and delivery payloads, enabling forged webhook events against victim organizations.	2026-06-19	6.5	CVE-2026-56079
Capgo--Capgo	Capgo before 12.128.2 contains an authorization bypass vulnerability in the /build/status and /build/logs endpoints that allows attackers to access build jobs belonging to different applications by supplying a mismatched app_id and job_id combination. Limited API keys restricted to a single app can retrieve build status and logs from other apps by providing an authorized app_id while using a job_id from an unauthorized app, exposing sensitive build information including logs, metadata, and potentially credentials.	2026-06-21	6.5	CVE-2026-56229

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Capgo--Capgo	Capgo before 12.128.2 contains a broken row level security policy in the org_users table that allows authenticated users to elevate privileges from admin to super_admin. Attackers can exploit the insufficient RLS enforcement to gain unauthorized super_admin access and compromise system security.	2026-06-21	6.5	CVE-2026-56251
Capgo--Capgo	Capgo before 12.128.2 contains an authorization bypass vulnerability in webhook management endpoints that allows non-expiring API keys to bypass the require_apikey_expiration organization policy. The checkWebhookPermission function fails to call apikeyHasOrgRightWithPolicy, enabling attackers with legacy non-expiring keys to list, create, and delete webhooks despite explicit organizational policy requiring key expiration.	2026-06-20	6.3	CVE-2026-56295
Capgo--Capgo	Capgo before 12.128.2 contains an authorization bypass vulnerability in the public.upsert_version_meta SECURITY DEFINER function exposed via PostgREST RPC, allowing unauthenticated attackers to insert arbitrary rows into version_meta for any app_id. Attackers can exploit this by calling the RPC endpoint with a public anon key to poison storage metrics, causing persistent false data in dashboards and triggering incorrect alerts across victim applications.	2026-06-20	5.3	CVE-2026-56213
Capgo--Capgo	Capgo before 12.128.2 fails to strip EXIF metadata including GPS geolocation data from uploaded images, allowing information disclosure. Attackers can download uploaded images and extract precise latitude and longitude coordinates revealing user physical location at capture time.	2026-06-20	5.3	CVE-2026-56218
Capgo--Capgo	Capgo before 12.128.2 contains a server-side request forgery vulnerability in webhook URL validation that allows loopback and internal addresses. Organization admins can configure webhooks pointing to localhost or 127.0.0.1, and when triggered, the backend performs outbound requests to these addresses with error responses disclosed to users.	2026-06-20	5.4	CVE-2026-56227
Capgo--Capgo	Capgo before 12.128.2 contains an information disclosure vulnerability in the unauthenticated /replication endpoint that exposes internal PostgreSQL replication telemetry including slot names and WAL LSN positions. Attackers can access this endpoint without authentication to retrieve sensitive infrastructure details such as replication slot names, confirmed_flush_lsn, restart_lsn values, and database error messages for reconnaissance purposes.	2026-06-20	5.3	CVE-2026-56282
Capgo--Capgo	Capgo before 12.128.2 contains an authentication bypass vulnerability in the /build/upload/:jobId/* endpoint that allows unauthenticated attackers to trigger consistent 500 errors. Remote attackers can send OPTIONS requests to bypass authentication middleware and invoke tusProxy logic with invalid credentials, enabling trivial request flooding and denial of service.	2026-06-21	5.3	CVE-2026-56299
Capgo--Capgo	Capgo before 12.128.2 fails to enforce a maximum value on the minimum password length field in its password policy configuration. An authenticated organization administrator can set an extremely large numeric value (e.g., billions of characters) as the minimum password length, making compliance impossible for all organization members. Once the policy is enabled, users (including administrators) are unable to change	2026-06-20	4.9	CVE-2026-56228

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	their passwords or access the organization, resulting in an organization-wide account lockout and application-level denial of service.			
Capgo--Capgo	Capgo before 12.128.2 contains an information disclosure vulnerability in the GET /statistics/app/:app_id endpoint that allows app-limited API keys to distinguish existing sibling app IDs through differential error responses. Attackers can enumerate real app IDs outside their allowed scope by observing 500 PGRST116 errors for inaccessible apps versus 401 errors for nonexistent apps, breaking tenant isolation.	2026-06-20	4.3	CVE-2026-56319
Capgo--Capgo	Capgo before 12.128.2 contains an open redirect vulnerability in the confirm-signup endpoint that allows attackers to redirect users to arbitrary external websites. The confirmation_url parameter is not validated, enabling attackers to craft malicious links for phishing and credential harvesting attacks.	2026-06-20	4.7	CVE-2026-56332
capgo--cli	Capgo CLI before 12.128.2 contains arbitrary file overwrite vulnerabilities in login and build credentials operations that follow symlinks without validation. Attackers can create malicious symlinks in repositories to overwrite arbitrary files or expose credentials with world-readable permissions when developers run the CLI.	2026-06-21	6.1	CVE-2026-56236
carrierwaveuploader--carrierwave	CarrierWave is a framework to upload files from Ruby applications. In versions prior to 2.2.7 and 3.1.3, the content_type_denylist check fails to escape regex metacharacters in string entries, causing the denylist to silently not match the content types it is intended to block. In lib/carrierwave/uploader/content_type_denylist.rb:57, denylist entries are interpolated directly into a regex without Regexp.quote or anchoring, so an entry such as image/svg+xml becomes the pattern /image\/svg+xml/, in which + is treated as a quantifier rather than a literal character and therefore never matches the real MIME type image/svg+xml. This is inconsistent with the allowlist implementation, which correctly applies both Regexp.quote and a \A anchor. Other content types containing regex metacharacters, such as application/xhtml+xml, are affected as well. As a result, any application that relies on content_type_denylist to block image/svg+xml, most commonly to prevent stored XSS, is silently unprotected. An attacker can upload an SVG file containing arbitrary JavaScript; if the application serves that SVG inline from its own origin, the script executes in the victim's browser, resulting in stored XSS. This issue has been fixed in versions 2.2.7 and 3.1.3.	2026-06-16	4.7	CVE-2026-44587
Cisco--Cisco Catalyst SD-WAN Manager	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an authenticated, remote attacker to create a file or overwrite any file on the filesystem of an affected system. This vulnerability exists because the affected software does not properly validate user-supplied input during a file upload process. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected API endpoint of the affected system. A successful exploit could allow the attacker to create or overwrite any file on the underlying operating system. This file could later be used to elevate to root. To exploit this vulnerability, the attacker must have valid credentials with at least a lower-privileged, single-task user account.	2026-06-15	6.5	CVE-2026-20262
Cisco--Cisco Crosswork	A vulnerability in the web-based management interface of Cisco Crosswork Network Controller could allow an authenticated, remote attacker	2026-06-17	6.3	CVE-2026-20220

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Network Change Automation	to execute arbitrary commands on an affected device. This vulnerability is due to insufficient input validation in the configuration template engine of the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system in limited areas of the file system. This vulnerability affects only areas of the operating system for which the template user has write permissions. To exploit this vulnerability, the attacker must have valid template user credentials with write permissions. Template users with read permissions cannot exploit this vulnerability.			
Cisco--Cisco Umbrella Insights Virtual Appliance	A vulnerability in the vmadmin CLI of Cisco Umbrella Virtual Appliance could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied commands. An attacker with vmadmin privileges could exploit this vulnerability by using certain commands at the CLI. A successful exploit could allow the attacker to elevate privileges to root.	2026-06-17	6	CVE-2026-20246
Cisco--Cisco Webex App	A vulnerability in the browser-based version of Cisco Webex App could have allowed an unauthenticated, remote attacker to redirect users to a malicious webpage. Cisco has addressed this vulnerability in the Cisco Webex App, and no customer action is needed. This vulnerability existed due to improper input validation of URL parameters in an HTTP request. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by persuading a user to click a crafted URL. A successful exploit could have allowed the attacker to redirect a user to a malicious website.	2026-06-17	4.3	CVE-2026-20178
Client Portal Ltd.- -Client Portal (Pro)	CP Client Arbitrary File Download in Client Portal (Pro) <= 5.6.2 versions.	2026-06-17	6.5	CVE-2026-40724
Cloud Foundry Foundation-- bpm-release	setupBpmLogs follows symlink for bpm.log open and chown - container-to-host privilege escalation via /etc/shadow. A compromised process inside a bpm container can cause root to chown an arbitrary host file to vcap and append bpm JSON log lines to it. The chown alone lets the attacker take ownership of /etc/shadow and read every password hash on the host via the read-only /etc bind mount. This is a container-to-host confidentiality break affecting every bpm-managed job. Affected versions: bpm-release, all versions prior to v1.4.30.	2026-06-18	6.1	CVE-2026-47833
Cloudflare-- Quiche	Cloudflare Quiche was affected by 2 use-after-free vulnerabilities in the connection ID iterator FFI functions. The "quiche_connection_id_iter_next" and "quiche_conn_retired_scid_next" functions would return a pointer to a "ConnectionId" to the applications via function arguments, but the owned "ConnectionId" would be dropped at the end of those functions' scope. Only applications using those FFI functions are affected. The FFI API is disabled by default by a build-time feature flag. Impact If unpatched, an application calling the affected FFI functions will dereference freed memory. The most likely outcome is undefined behavior leading to a process crash (denial of service). Depending on allocator state, the read may also return adjacent heap contents, resulting in limited information disclosure or incorrect connection identifier handling. Mitigation Users are requested to upgrade	2026-06-19	5.6	CVE-2026-11941

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to quiche 0.29.2 which is the earliest version containing the fix for this issue.			
codepeople--Appointment Booking Calendar	The Appointment Booking Calendar plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 1.4.01. This is due to insufficient authorization and missing per-calendar ownership checks in the cpabc_appointments_calendar_load2() function, which is reachable via the cpabc_calendar_load2=1 query parameter in wp-admin and only checks is_admin() && current_user_can('edit_posts'), a capability available to Contributor-level users and above. This makes it possible for authenticated attackers with Contributor-level access and above to supply an arbitrary calendar ID via the id parameter and extract customer booking information, including email addresses, names, phone numbers, booking times, and comments, from any calendar managed by the plugin.	2026-06-18	4.3	CVE-2026-12111
Comfast--CF-WR631AX V3	A flaw has been found in Comfast CF-WR631AX V3 up to 2.7.0.8. This issue affects the function system of the file /cgi-bin/mbox-config?section=ping_config of the component API Endpoint. This manipulation of the argument destination causes os command injection. The attack is possible to be carried out remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	6.3	CVE-2026-12814
contrid--Slideshow Gallery LITE	The Slideshow Gallery LITE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'alwaysauto' shortcode attribute in all versions up to, and including, 1.8.5. This is due to insufficient input sanitization and output escaping on user-supplied attributes. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-18	6.4	CVE-2026-2021
collabsio--coolify	A vulnerability has been found in collabsio coolify 4.0.0. Impacted is an unknown function of the component Image Name Handler. Such manipulation leads to os command injection. The attack may be performed from remote. The vendor was contacted early about this disclosure but did not respond in any way. The changelog for 4.1.2 mentions "[i]mproved image, branch, proxy, and deployment input validation".	2026-06-21	6.3	CVE-2026-12815
Cotonti--Cotonti	Cotonti 1.0.0 (master branch, commit f43f1fc3) is vulnerable to Cross-Site Request Forgery in the Personal File Storage (PFS) module. In modules/pfs/inc/pfs.editfolder.php, the folder update action ('a=update') updates folder metadata (title, description, public/gallery flags) without calling cot_check_xg() to validate the anti-CSRF token. A remote attacker who lures an authenticated user into visiting a malicious page can force the browser to submit a forged request that modifies the victim's folder metadata, including making a private folder public.	2026-06-18	5.4	CVE-2026-55745
coturn--coturn	Coturn is a free open source implementation of TURN and STUN Server. Versions prior to 4.11.0 contain a stored cross-site scripting (XSS) vulnerability in the web-admin HTTPS interface. An attacker who can create a TURN allocation with a crafted USERNAME value can inject HTML/JavaScript that executes when an authenticated web-admin user views the TURN session list. In configurations using anonymous TURN	2026-06-18	5.4	CVE-2026-43915

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	access (--no-auth), this may be exploitable without TURN credentials. In authenticated deployments, exploitation requires valid TURN credentials or control over a provisioned username. This issue has been fixed in version 4.11.0.			
craftcms--cms	Craft CMS from 4.0.0-RC1 contains an authenticated path traversal vulnerability in the assets/icon endpoint where the extension parameter is not validated before file existence checks. Attackers can bypass extension validation by passing traversal sequences that resolve to existing SVG files, allowing local file read access.	2026-06-21	6.5	CVE-2026-56394
craftcms--cms	Craft CMS from version 5.0.0-RC1 contains a stored cross-site scripting vulnerability in the User Permissions page where user group names are rendered without proper HTML escaping. Attackers with admin access can inject arbitrary JavaScript via the user group name field that executes when other users view or edit permissions.	2026-06-21	4.8	CVE-2026-56381
craftcms--cms	Craft CMS contains a stored cross-site scripting (XSS) vulnerability in the editableTable.twig component when using the 'Row Heading' column type. The application fails to sanitize input within row heading default values, allowing an attacker with an administrator account (with allowAdminChanges enabled) to inject arbitrary JavaScript that executes when another user views a page containing the affected table field. Affected versions are >= 4.5.0-beta.1 through 4.16.18 and >= 5.0.0-RC1 through 5.8.22; fixed in 4.16.19 and 5.8.23.	2026-06-21	4.8	CVE-2026-56383
craftcms--cms	Craft CMS contains a missing authorization vulnerability in the assets/preview-thumb endpoint. A Control Panel user without permission to view a target private asset can call the endpoint with an attacker-controlled assetId and receive preview HTML containing a signed fallback transform preview link for that private asset, because no asset-view permission check is performed before preview generation. This affects versions >= 4.0.0-RC1, <= 4.17.7 and >= 5.0.0-RC1, <= 5.9.13, and is fixed in 4.17.8 and 5.9.14.	2026-06-21	4.3	CVE-2026-56384
craftcms--cms	Craft CMS versions >= 5.0.0-RC1, <= 5.9.13 and >= 4.0.0-RC1, <= 4.17.7 contain an authorization bypass in the assets/preview-file endpoint. The action does not enforce per-asset view authorization before returning preview content, allowing an authenticated low-privileged user to supply a controlled assetId for an asset they are not permitted to view and still receive preview response data (previewHtml), including a private preview image route containing the target private assetId. Fixed in 5.9.14 and 4.17.8.	2026-06-21	4.3	CVE-2026-56385
craftcms--cms	Craft CMS 4.x (>= 4.0.0-RC1, < 4.17.0-beta.1) and 5.x (>= 5.0.0-RC1, < 5.9.0-beta.1) contain multiple stored cross-site scripting vulnerabilities where settings names and field option labels are rendered without sanitization (e.g., via the checkbox.twig template, which used {{ label raw }}). An authenticated administrator (with allowAdminChanges enabled) can inject malicious payloads into section names, volume names, user group names, global set names, generated field names, checkbox/radio option labels, and custom source labels, causing arbitrary JavaScript to execute in other users' control-panel sessions. Fixed in 4.17.0-beta.1 and 5.9.0-beta.1.	2026-06-21	4.8	CVE-2026-56393

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
creativethemeshq--Blocksy Companion	The Blocksy Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.1.45 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2026-06-19	4.4	CVE-2026-12430
creavi--Creavi Appointment Booking Calendar	The Appointment Booking Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via custom booking field labels in all versions up to, and including, 1.4.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-19	6.4	CVE-2026-1856
deepakkite--Secure Client Portal and Private File Sharing Plugin User Private Files	The File Sharing & Download Manager - User Private Files plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'fldr_ttl' parameter in all versions up to, and including, 2.1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-16	6.4	CVE-2026-10093
Dell--Peripheral Manager	Dell Peripheral Manager, versions prior to 1.7.3, contain an uncontrolled search path element vulnerability. An attacker could potentially exploit this vulnerability through preloading malicious dll., leading to arbitrary code execution.	2026-06-16	6.7	CVE-2024-22447
Dell--Peripheral Manager	Dell Peripheral Manager, versions from 1.5.1 to 1.7.2, contain an uncontrolled search path element vulnerability. An attacker could potentially exploit this vulnerability through preloading malicious executable, leading to arbitrary code execution.	2026-06-16	6.7	CVE-2024-22451
Dell--PowerFlex	Dell PowerFlex Manager, version(s) [Versions], contain(s) an Improper Access Control vulnerability. A low privileged attacker with adjacent network access could potentially exploit this vulnerability, leading to Elevation of privileges and Unauthorized access.	2026-06-17	5.7	CVE-2026-35067
Dell--PowerFlex	Dell PowerFlex Manager, version(s) [Versions], contain(s) an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with adjacent network access could potentially exploit this vulnerability, leading to Script injection.	2026-06-17	5.7	CVE-2026-35069
Dell--PowerFlex	Dell PowerFlex Manager, version(s) [Versions], contain(s) an Improper Access Control vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to denial of service.	2026-06-17	4.3	CVE-2026-35162
Dell--PowerFlex	Dell PowerFlex Manager, version(s) 4.6.0.1, contain(s) an Use of a Broken or Risky Cryptographic Algorithm vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure and Information tampering.	2026-06-17	4.8	CVE-2026-40641
Dell--PowerFlex Manager	Dell PowerFlex Manager, versions prior to 4.5.1.1, contain an improper certificate validation vulnerability. A remote unauthenticated attacker	2026-06-17	6.5	CVE-2024-47477

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could potentially exploit this vulnerability leading to man-in-the-middle attack in tandem with DNS cache poisoning.			
Dell--PowerFlex rack	Dell PowerFlex rack, version(s) RCM 3.7/3.7, contain(s) a Host Header Injection vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability to trigger redirections.	2026-06-17	4.3	CVE-2025-32748
Dell--PowerStore	PowerStore contains a Stored Cross-Site Scripting Vulnerability in the PowerStore Manager. A remote authenticated low-privileged malicious actor could potentially exploit this vulnerability, it could lead to script execution in the client browser.	2026-06-16	5.4	CVE-2024-30476
dijitul--Fancy Testimonials	The Fancy Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'author' shortcode attribute in the 'testimonial' shortcode in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-18	6.4	CVE-2026-8039
Discuz!--Discuz! X5.0	Discuz! X5.0 releases 20260320 through 20260610 contains a CAPTCHA bypass vulnerability that allows unauthenticated remote attackers to defeat challenge controls by exploiting limited complexity and predictable character sets in generated CAPTCHA images. Attackers can train a custom optical character recognition model against collected CAPTCHA samples to reliably predict challenge text, bypassing protections on login, registration, and other functionality from automated abuse.	2026-06-15	6.5	CVE-2026-49953
dokaninc--Dokan: AI Powered WooCommerce Multivendor Marketplace Solution Build Your Own Amazon, eBay, Etsy	The Dokan: AI Powered WooCommerce Multivendor Marketplace Solution - Build Your Own Amazon, eBay, Etsy plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.0.3 via the change_order_status, add_order_note, delete_order_note, add_shipping_tracking_info, grant_access_to_download, and revoke_access_to_download AJAX handlers due to missing ownership validation on a user-controlled order ID key. This makes it possible for authenticated attackers, with custom vendor-level access and above, to modify the status of arbitrary orders, add attacker-controlled notes to any order (including customer-facing notes that trigger WooCommerce notification emails to buyers), delete any order note or WordPress comment by ID regardless of ownership, inject fake shipping tracking information on any order, and grant or revoke downloadable-product permissions on any order in the marketplace. Critically, nonce validity is not a barrier to exploitation: each of these AJAX handlers generates and embeds its nonce on the authenticated vendor's own dashboard order pages (e.g., /dashboard/orders/?order_id=OWN_ORDER_ID), which the attacker legitimately controls. The attacker harvests a valid nonce from their own order detail page and replays it against a victim order ID - the nonce only proves the request originates from a logged-in session, not that the order belongs to that vendor. This directly rebuts the prior rejection reasoning that 'users cannot generate valid nonces on command': vendor users can and do generate valid nonces on demand simply by loading their own dashboard pages. Source-code analysis confirmed the vulnerable code path is present and unpatched through version 5.0.1.	2026-06-18	4.3	CVE-2026-10023

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dwbooster--Booking Calendar Contact Form	WordPress Booking Calendar Contact Form 1.0.23 contains privilege escalation and stored cross-site scripting vulnerabilities that allow authenticated users to modify plugin options and inject malicious scripts by failing to verify user privileges and sanitize input parameters. Attackers with subscriber-level accounts can inject XSS payloads through parameters like price, name, calendar_language, and email_confirmation_to_user via admin-ajax.php and admin.php endpoints to execute arbitrary JavaScript in administrator browsers.	2026-06-15	6.4	CVE-2016-20070
dwbooster--CP Polls	WordPress CP Polls 1.0.8 contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized actions on behalf of authenticated users. Attackers can craft malicious HTML pages that execute unwanted poll operations when administrators visit the page while logged in.	2026-06-15	4.3	CVE-2016-20067
Edimax--BR-6478AC V2	A vulnerability was found in Edimax BR-6478AC V2 1.23. This affects the function setWAN of the file /goform/setWAN of the component POST Request Handler. The manipulation of the argument pppUserName/pptpUserName/L2TPUserName results in command injection. It is possible to launch the attack remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	6.3	CVE-2026-12807
Edimax--BR-6478AC V2	A vulnerability was determined in Edimax BR-6478AC V2 1.23. This impacts the function stainfo of the file /goform/stainfo of the component POST Request Handler. This manipulation of the argument interface causes command injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	6.3	CVE-2026-12808
Edimax--BR-6478AC V2	A vulnerability was identified in Edimax BR-6478AC V2 1.23. Affected is the function wiz_5in1_redirect of the file /goform/wiz_5in1_redirect of the component POST Request Handler. Such manipulation of the argument newpass leads to command injection. The attack can be launched remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	6.3	CVE-2026-12809
Edimax--BR-6478AC V2	A security flaw has been discovered in Edimax BR-6478AC V2 1.23. Affected by this vulnerability is the function mp of the file /goform/mp of the component POST Request Handler. Performing a manipulation of the argument command results in command injection. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	6.3	CVE-2026-12810
eeemitch--Simple File List	The Simple File List plugin for WordPress is vulnerable to unauthorized file operations due to a missing authorization check on the 'frontmanage' shortcode attribute in all versions up to, and including, 6.3.7. This makes it possible for authenticated attackers, with contributor-level access and above, to perform arbitrary file operations including deletion, move, folder creation, and download. An attacker can create a draft post containing the 'eeSFL' shortcode, render it via the post preview endpoint to harvest the nonce needed to authorize the operations, and then submit file operation requests that bypass the intended authorization checks in includes/ee-list-ops-bar-process.php.	2026-06-20	6.5	CVE-2026-12119

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
eLightUp--Meta Box WordPress Custom Fields Framework	Contributor Arbitrary File Deletion in Meta Box - WordPress Custom Fields Framework <= 5.11.1 versions.	2026-06-15	6.8	CVE-2026-39468
equalizedigital--Equalize Digital Accessibility Checker WCAG, ADA, EAA and Section 508 compliance	The Equalize Digital Accessibility Checker - WCAG, ADA, EAA and Section 508 compliance plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.42.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with author-level access and above, to dismiss, ignore, or restore accessibility audit issue records belonging to posts they are not permitted to edit by supplying an issue from their own post as an authorization token to affect matching issues across the entire site. An Author-level user can exploit this by passing largeBatch=true on a dismiss-issue request referencing one of their own post's issues, causing the handler to bulk-modify all site-wide accessibility issues sharing the same 'object' value - including those belonging to administrator-owned posts.	2026-06-18	4.3	CVE-2026-9199
eventkoi--Event Koi Lite Events Calendar, Event Management, RSVP, and Tickets	The Event Koi Lite - Events Calendar, Event Management, RSVP, and Tickets plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.3.13.1 via the get_events. This makes it possible for unauthenticated attackers to extract sensitive data including virtual meeting URLs, physical location data, latitude/longitude coordinates, Google Maps links, and RSVP configuration belonging to draft, pending, and private events that are otherwise inaccessible via public URLs.	2026-06-18	5.3	CVE-2026-10029
Extend Themes--Skyline WP	Cross-Site request forgery (CSRF) vulnerability in Extend Themes Skyline WP allows Cross Site Request Forgery. This issue affects Skyline WP: from n/a through 1.0.10.	2026-06-17	4.3	CVE-2024-34810
F5--NGINX Gateway Fabric	When NGINX Gateway Fabric is configured using GRPCRoutes, an authenticated, remote attacker with permission to create or modify GRPCRoute resources can cause the NGINX Gateway Fabric control plane to terminate by sending undisclosed GRPCRoute configurations containing backendRef filters. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-06-17	6.5	CVE-2026-32682
F5--NGINX Open Source	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_charset_module module. When content is served or proxied through a location block with both source_charset utf-8; and a charset directive (for example, charset koi8-r;) configured, remote, unauthenticated attackers can send requests (in conjunction with conditions beyond their control) to cause a heap buffer over-read in the NGINX worker process, leading to limited disclosure of memory or a restart. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-06-17	4.8	CVE-2026-48142
fdflyer--DroneAware-Node-Releases	DroneAware is a drone detection platform. The centralized DroneAware server backing droneaware.io was vulnerable to an account pre-hijacking attack in which an attacker could register an account using a victim's email address with an attacker-controlled password before the victim completed account activation. When the legitimate owner later activated the account, either by clicking the email verification link or by logging in via	2026-06-17	6.8	CVE-2026-48117

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Google SSO, the attacker-set password became fully valid, enabling silent and persistent account takeover without any notification to the victim. The vulnerability was fixed server-side on 2025-05-20; no user action is required. Node binaries and self-hosted detection nodes are not affected. There are no workarounds; the fix was deployed server-side and no client-side mitigation is applicable.			
fireplugins--FireBox Popups Increase Sales and Grow Your Email List	The FireBox Popups - Increase Sales and Grow Your Email List plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.1.7 via the 'form_id' parameter. This makes it possible for unauthenticated attackers to extract download a full CSV export of all form submissions - including any personally identifiable information submitted by users - for any arbitrary form_id.	2026-06-18	5.3	CVE-2026-12120
Flowise--Flowise	Flowise before 3.0.8 contains a cross-site scripting (XSS) vulnerability caused by insufficient input filtering in chat messages and custom agent functions. An attacker can inject malicious JavaScript by sending an iframe payload (e.g., <iframe src="javascript:alert(document.cookie)">) in a chat box, or by having a custom agent function return an XSS payload from an external website. The injected script executes in the victim's browser, enabling theft of cookies and session data.	2026-06-20	6.1	CVE-2025-71331
FlowiseAI--Flowise	A vulnerability was determined in FlowiseAI Flowise up to 3.1.2. The impacted element is an unknown function of the file packages/components/nodes/documentloaders/S3/S3.ts of the component S3 Document Loader. Executing a manipulation can lead to path traversal. It is possible to launch the attack remotely. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	6.3	CVE-2026-12821
FluxBuilder--MStore API	Authentication Bypass Using an Alternate Path or Channel vulnerability in FluxBuilder MStore API allows Password Recovery Exploitation. This issue affects MStore API: from n/a through 4.18.4.	2026-06-17	6.5	CVE-2026-54817
FolioVision--FV Flowplayer Video Player	Subscriber Cross Site Scripting (XSS) in FV Flowplayer Video Player < 7.5.51.7212 versions.	2026-06-15	6.5	CVE-2026-49773
geoserver--org.geoserver.web:gs-web-app	GeoServer is an open source server that allows users to share and edit geospatial data. Prior to versions 2.26.4 and 2.27.3, a GeoServer that uses 'ENTITY_RESOLUTION_ALLOWLIST' may allow attacker to perform unauthenticated Server-Side Request Forgery (SSRF). This vulnerability requires that GeoServer is set up to use a proxy base URL and the 'ENTITY_RESOLUTION_ALLOWLIST' (default since 2.25.0). Versions 2.26.4 and 2.27.3 contain a fix. GeoServer installations are only affected by this vulnerability if they use a proxy base URL that does not contain a URL path or end with a slash. If the proxy base URL does not contain a path, adding a slash to the end of the URL will mitigate this vulnerability.	2026-06-18	6.5	CVE-2025-58175
gitroomhq--postiz-app	Postiz is an AI social media scheduling tool. Versions prior to 2.21.8 contained an unauthenticated endpoint that accepted a signed token and applied subscription-enforcement side effects to the organization referenced in that token's claims, without verifying the token's intended purpose. The endpoint, /public/modify-subscription, could not change the persisted subscription tier, but it did execute enforcement-related side effects on the caller's own organization, including adjusting team-member enablement state, disabling integrations exceeding the asserted plan's	2026-06-16	4.8	CVE-2026-48783

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	limits, and resetting the scheduled-post cron when the asserted plan was the free tier. Impact is limited to the attacker's own organization and cannot be redirected at other tenants through this endpoint. This issue has been fixed in version 2.21.8.			
GNOME-- Evolution Data Server	A flaw was found in evolution-data-server. Inconsistent comparison logic in the addressbook file backend allows a Flatpak application with D-Bus access to craft a malicious URI containing directory traversal sequences. This URI is stored without proper validation during contact creation or modification. Later, during contact deletion, the URI is processed with a less strict check, leading to the deletion of arbitrary files on the host filesystem. This could potentially include critical Flatpak override files.	2026-06-16	5.6	CVE-2026-2604
Government Accountability Office--Electronic Protest Docketing System (EPDS)	The U.S. Government Accountability Office (GAO) Electronic Protest Docketing System (EPDS) and Civilian Board of Contract Appeals (CBCA) Electronic Docketing System (EDS) expose sensitive account information through the 'update-profile/' API endpoint. A remote, unauthenticated attacker can submit a request containing an arbitrary 'user_id' parameter and receive a JSON response containing account-specific information, including the associated email address.	2026-06-18	5.3	CVE-2026-54105
Government Accountability Office--Electronic Protest Docketing System (EPDS)	The U.S. Government Accountability Office (GAO) Electronic Protest Docketing System (EPDS) and Civilian Board of Contract Appeals (CBCA) Electronic Docketing System (EDS) do not validate X-Forwarded-For HTTP headers, allowing a remote attacker with compromised administrator credentials to bypass network access controls and log in.	2026-06-18	4.7	CVE-2026-54106
Grafana-- Enterprise Traces (GET)	A TraceQL query in Grafana Tempo with a large exemplars hint value can cause the Tempo instance to allocate an excessive amount of memory, resulting in an out-of-memory crash. This could allow an authenticated user to trigger a denial of service against the Tempo service.	2026-06-19	6.5	CVE-2026-27878
Greg Winiarski-- WPAdverts	Unauthenticated Broken Access Control in WPAdverts <= 2.3.0 versions.	2026-06-15	6.5	CVE-2026-40782
Grit42--Grit	A vulnerability was identified in Grit42 Grit up to 0.11.0. This issue affects the function Grit::Assays::DataTableEntity of the file modules/assays/backend/app/models/grit/assays/data_table_entity.rb. The manipulation leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	6.3	CVE-2026-12206
Groundhogg-- Groundhogg	Subscriber Broken Access Control in Groundhogg < 4.4.1 versions.	2026-06-15	6.5	CVE-2026-40793
Hackplayers-- evil-winrm	Evil-WinRM through 3.9, fixed in commit 6ecd570, contains a path traversal vulnerability in the download_dir() function that allows a rogue or compromised remote Windows server to write files outside the intended download directory by returning filenames with traversal sequences from Get-ChildItem command output that are passed unsanitized to File.join(). Attackers controlling the remote server can exploit this to overwrite sensitive client-side files such as SSH	2026-06-17	6.8	CVE-2026-55201

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authorized_keys or shell configuration files, achieving persistent access or privilege escalation on the client machine.			
hantle--liquidjs	LiquidJS is a Shopify/GitHub Pages compatible template engine written in pure JavaScript. Versions 10.25.7 and below are vulnerable to XSS through a flaw in the strip_html filter logic. The strip_html filter is intended to remove HTML tags from a string before rendering, and is widely used as an XSS sanitizer. The implementation uses a regex whose catch-all branch (<.*?>) does not match line terminators, so any HTML tag containing a \n or \r character passes through unmodified. An attacker who can place a newline inside a tag (e.g. <img\nsrc=x\nonerror=alert(1)>) bypasses sanitization entirely, since browsers treat newlines as whitespace within a tag and execute the resulting onerror/onload/etc. handler. Exploitation is possible for applications that both render attacker-controlled strings via {{ x strip_html }} to defend against HTML injection and do not separately HTML-escape that output (default behavior - outputEscape is unset by default). This issue has been fixed in version 10.26.0.	2026-06-17	6.1	CVE-2026-44644
hantle--liquidjs	LiquidJS is a Shopify/GitHub Pages compatible template engine written in pure JavaScript. In versions 10.25.7 and below, the renderLimit option can be fully bypassed by a {% for %} (or {% tablerow %}) tag whose body is empty. The renderLimit option is documented in docs/source/tutorials/dos.md as the mechanism that "mitigates this by limiting the time consumed by each render() call." The per-iteration time check is reached only when the body contains at least one template node, so a template such as {%- for i in (1..N) -%}{%- endfor -%} iterates the full collection without ever consulting renderLimit. With a configured renderLimit of 50 ms, a single parseAndRenderSync call has been observed to consume 2.26 seconds (~45x — over the limit) and scales linearly with N up to memoryLimit, allowing a low-privileged template author to wedge an event-loop thread for an attacker-chosen duration. Deployments that rely on a finite renderLimit for DoS protection (common in multi-tenant template-authoring environments) can still be forced by a single crafted template to monopolize a Node.js event-loop worker for attacker-controlled time, potentially stalling in-flight requests, with availability impact only. This issue has been fixed in version 10.26.0.	2026-06-17	6.5	CVE-2026-44645
hantle--liquidjs	LiquidJS is a Shopify/GitHub Pages compatible template engine written in pure JavaScript. In versions 10.25.7 and below, Context.spawn() creates a child Context for the {% render %} tag but does not propagate the parent context's resolved ownPropertyOnly value, resulting in a silent bypass. The new context re-derives ownPropertyOnly from opts.ownPropertyOnly (the instance-level option), silently discarding any RenderOptions.ownPropertyOnly override that was supplied to parseAndRender(). As a result, a developer who runs a Liquid instance with the backwards-compatible ownPropertyOnly:false and then locks down an untrusted render with parseAndRender(..., { ownPropertyOnly: true }) still leaks prototype-chain properties from inside any {% render %} partial. This is a distinct exploit surface from the previously identified array-filter variants (where, reject, group_by, find, find_index, has) - the underlying root cause in Context.spawn() is shared, but {% render %} is a separately reachable sink that needs no filter usage. This issue has been fixed in version 10.26.0.	2026-06-17	5.3	CVE-2026-44646

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
hashgraph--guardian	Hashgraph Guardian through 3.5.0, fixed in commit ba8c566, contains a stored cross-site scripting vulnerability that allows authenticated users with the STANDARD_REGISTRY role to inject malicious scripts by submitting a crafted companyName value via the branding configuration API endpoint. Attackers can exploit the unsanitized innerHTML assignment in the branding service to execute arbitrary JavaScript in the browser of every authenticated user on every page load.	2026-06-18	4.8	CVE-2026-22674
hcengineering--Huly Platform	A vulnerability has been found in hcengineering Huly Platform up to 0.7.0. Affected is the function getMailboxSecret of the file server/account/src/operations.ts of the component RPC Interface. The manipulation leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	4.3	CVE-2026-12212
hcengineering--Huly Platform	A vulnerability was found in hcengineering Huly Platform up to 0.7.0. Affected by this vulnerability is the function getAccountInfo of the file server/account/src/operations.ts of the component User Information Handler. The manipulation results in improper authorization. The attack may be launched remotely. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	4.3	CVE-2026-12213
HCL Software--ZIE	HCL ZIE for Web is affected by an Unrestricted File Upload vulnerability, If the server is configured to execute code, then it may be possible to obtain command execution on the server by uploading a file known as a web shell, which allows you to execute arbitrary code or operating system commands. For this attack to be successful, the file needs to be uploaded inside the Webroot, and the server must be configured to execute the code	2026-06-17	4.3	CVE-2025-59872
HCLSoftware--Verse for Android	The compose-rich-editor library (v1.0.0-rc14) used in HCL Verse for Android's rich text email composition fails to properly validate all HTML input thereby allowing malicious content to be executed in certain situations.	2026-06-19	6.3	CVE-2026-21768
henrikmelin--More Fields	WordPress More Fields Plugin 2.1 contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized actions by disabling CSRF token validation. Attackers can craft malicious web pages that trick logged-in administrators into adding or deleting custom fields and boxes on the Write/Edit page via POST and GET requests to the options-general.php endpoint.	2026-06-15	5.3	CVE-2016-20083
Henrique Dias--IMDb Profile Widget	WordPress IMDb Profile Widget 1.0.8 contains a local file inclusion vulnerability that allows unauthenticated attackers to read arbitrary files by manipulating the url parameter. Attackers can supply directory traversal sequences in GET requests to pic.php to access sensitive files like wp-config.php containing database credentials and configuration data.	2026-06-15	6.2	CVE-2016-20078
HKUDS--AI-Trader	A vulnerability was found in HKUDS AI-Trader up to 74caf996f78dcc0c657df8365c8544678a16e215. This affects an unknown part of the file /api/research/agents.csv of the component Research Export. Performing a manipulation results in information disclosure. Remote exploitation of the attack is possible. The exploit has been made public and could be used. This product follows a rolling release approach	2026-06-15	5.3	CVE-2026-12203

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	for continuous delivery, so version details for affected or updated releases are not provided. The patch is named 91a31aac1b0f4dbc6b8bef9f6eff0b7912e0bc65. Applying a patch is the recommended action to fix this issue. The vendor confirms: "Research export endpoints now require an authenticated agent with the research_exports capability".			
ILIAS--Learning Management System	A vulnerability was identified in ILIAS Learning Management System 11.0. This issue affects the function ilTrQuery::executeQueries of the file components/ILIAS/Tracking/classes/class.ilTrQuery.php of the component Learning Progress Tracking. Such manipulation of the argument troupe_table_nav leads to sql injection. It is possible to launch the attack remotely. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	4.7	CVE-2026-12789
info@welcart--Welcart e-Commerce	Unauthenticated Broken Access Control in Welcart e-Commerce <= 2.11.28 versions.	2026-06-15	6.5	CVE-2026-49775
Inisev--Social Media & Share Icons	: Missing Authorization vulnerability in Inisev Social Media & Share Icons allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Social Media & Share Icons: from n/a through 2.8.6.	2026-06-17	4.3	CVE-2024-31435
IObit--Malware Fighter	A flaw has been found in IObit Malware Fighter up to 13.2.0. Affected by this vulnerability is an unknown functionality of the component DLL Handler. This manipulation causes permission issues. The attack requires local access. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	5.3	CVE-2026-12201
Iqonic Design--KiviCare	Subscriber Insecure Direct Object References (IDOR) in KiviCare <= 4.2.1 versions.	2026-06-15	6.3	CVE-2026-40792
j_3rk--Video Conferencing with Zoom	The Video Conferencing with Zoom plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.6.7. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to obtain the site's Zoom SDK API key and a freshly-signed JWT that can be used with the Zoom Web SDK to join any Zoom meeting associated with those credentials without a legitimate invitation.	2026-06-16	5.3	CVE-2026-6964
jamie--Dharma Booking	WordPress Dharma Booking 2.28.3 and earlier contains a local file inclusion vulnerability that allows unauthenticated attackers to include arbitrary files by manipulating the gateway parameter. Attackers can supply file paths with directory traversal sequences or null byte injection to the gateway parameter in process.php to read sensitive files like configuration and system files.	2026-06-15	6.2	CVE-2016-20079
Jegstudio--Startupzy	Missing Authorization vulnerability in Jegstudio Startupzy startupzy allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Startupzy: from n/a through 1.1.1.	2026-06-17	4.3	CVE-2024-33685
Jetmonsters--JetFormBuilder	Subscriber Privilege Escalation in JetFormBuilder <= 3.6.1 versions.	2026-06-17	6.8	CVE-2026-54196

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
igwhite33--WP Google Review Slider	Unauthenticated Cross Site Scripting (XSS) in WP Google Review Slider <= 18.0 versions.	2026-06-15	6.3	CVE-2026-39451
Joomtech--Easy Shop	Joomla! Component Easy Shop 1.2.3 contains a local file inclusion vulnerability that allows unauthenticated attackers to read arbitrary files by supplying base64-encoded file paths. Attackers can send GET requests to index.php with the option parameter set to com_easyshop, task set to ajax.loadImage, and a base64-encoded file path in the file parameter to retrieve sensitive files like configuration.php and system files.	2026-06-19	6.2	CVE-2019-25760
jsonata-js--jsonata	A weakness has been identified in jsonata-js jsonata up to 2.2.0. The affected element is the function createFrame of the file src/jsonata.js of the component Function Binding Frame System. This manipulation causes improperly controlled modification of object prototype attributes. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	5.3	CVE-2026-12208
Jthemes--Genemy	Subscriber Broken Access Control in Genemy <= 1.6.6 versions.	2026-06-16	6.5	CVE-2025-69137
juice-shop--multi-juicer	MultiJuicer is used to run separate Juice Shop instances on a central kubernetes cluster without the need for local instances. In versions 8.0.0 through 10.0.0, the team join endpoint (POST /multi-juicer/api/teams/{team}/join) accepted requests with any Content-Type, including text/plain. Because that content type does not trigger a CORS preflight, an attacker could host a cross-site HTML form that auto-submits to the endpoint and forces a victim's browser to log in as the attacker's team. A successful, undetected attacker can cause victims to unwittingly solve Juice Shop challenges under the attacker's team identity. In a CTF context this lets the attacker inflate their team's score using other players' activity, and any sensitive data the victim enters into "their" Juice Shop ends up in the attacker's instance. The vulnerability is exploitable without any prior authentication; the victim only needs to visit a page the attacker controls while having network access to the MultiJuicer deployment. SameSite=Strict on the session cookie does not mitigate this, because the attack plants a new cookie rather than relying on an existing one. This issue was fixed in version 10.0.1.	2026-06-15	4.3	CVE-2026-48518
KaymeePhotography--Photocart Link	WordPress Plugin Photocart Link 1.6 contains a local file inclusion vulnerability that allows unauthenticated attackers to read arbitrary files by exploiting insufficient input validation in decode.php. Attackers can supply base64-encoded file paths in the 'id' parameter to the decode.php endpoint to retrieve sensitive files like wp-config.php containing database credentials and configuration data.	2026-06-15	6.2	CVE-2016-20077
kestra-io--kestra	Kestra is an open-source, event-driven orchestration platform. Prior to versions 1.3.19, 1.2.19, 1.1.19, and 1.0.43, Kestra task `inputFiles` writes rendered file names directly under the task working directory. When a flow forwards untrusted execution or webhook data into an `inputFiles` file name, a caller can use `../` path segments to create or overwrite files outside that task working directory on the worker filesystem. Versions 1.3.19, 1.2.19, 1.1.19, and 1.0.43 patch the issue.	2026-06-19	6.5	CVE-2026-48129

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
King Addons-- King Addons for Elementor	Subscriber Cross Site Scripting (XSS) in King Addons for Elementor <= 51.1.62 versions.	2026-06-15	6.5	CVE-2026-48870
Kludex--starlette	Starlette is a lightweight ASGI framework/toolkit. In versions 1.0.1 and below, when dispatching a request, HTTPEndpoint selects the handler by lowercasing the HTTP method and looking it up as an attribute with getattr, without restricting the lookup to a known set of HTTP verbs. When an HTTPEndpoint subclass is registered through Route(...) without an explicit methods= argument, the route does not constrain the method and every method reaches the endpoint. If a non-standard HTTP method whose lowercased name matches an attribute on the endpoint subclass reaches the endpoint, that attribute is invoked as if it were a request handler. An attacker can use this to reach methods that were never meant to be HTTP handlers, such as internal helpers, without the authorization checks applied by the intended public handler. An application (including Starlette-based frameworks like FastAPI) is affected if it registers an HTTPEndpoint subclass via Route(...) without explicitly setting methods=, and that subclass includes extra methods named like non-standard HTTP verbs that take one request argument and return a response. This issue has been fixed in version 1.1.0.	2026-06-17	5.3	CVE-2026-48817
kortix-ai--suna	A weakness has been identified in kortix-ai suna up to 0.8.38. Affected by this issue is the function router.replace/router.push of the file apps/frontend/src/app/auth/page.tsx of the component Auth Endpoint. Executing a manipulation of the argument returnUrl can lead to cross site scripting. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 0.8.39 can resolve this issue. This patch is called f5dec7aa0c1b8fa0125938f292c0f2430ca75f6c. It is advisable to upgrade the affected component. The researcher explains: "The issue was fixed in v0.8.39 without notifying the wider user base via a security disclosure."	2026-06-21	4.3	CVE-2026-12811
langchain-ai-- langchain-ai	LangGraph Python SDK is used to connect to running LangGraph API servers, manage assistants, threads and stream runs from Python applications. Versions 0.3.14 and prior have unsafe URL path construction through unsanitized caller-supplied identifier values used in HTTP request paths for resource operations. Without sanitization of those values, identifiers that contain characters with special meaning in URL paths could cause the resulting request to address a different resource (and potentially a different resource type) than the SDK method's call site indicates. In deployments where the SDK receives identifier values that originate from untrusted sources, this could result in unintended access, modification, or deletion of resources beyond the calling user's authorization scope. This issue is most consequential in deployments that forward end-user-supplied values directly into SDK identifier parameters without first validating them against an expected format (such as a UUID), and rely on URL-prefix-based authorization at an upstream layer (reverse proxy, edge gateway, WAF), where the authorization decision is made on the SDK call's intended path rather than on the final delivered request path. The issue has been fixed in version 0.3.15.	2026-06-16	4.2	CVE-2026-48776
langchain-ai-- langgraph	LangGraph SQLite Checkpoint is an implementation of LangGraph CheckpointSaver that uses SQLite DB (both sync and async, via aiosqlite). In versions 4.1.0 and prior, the JsonPlusSerializer can reconstruct Python	2026-06-16	6.8	CVE-2026-48775

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	objects from JSON checkpoint payloads. Under conditions where someone could modify checkpoint bytes at rest in the backing store, the deserialization path could reconstruct objects beyond what the application expects, which could in turn result in code execution at checkpoint load time. This is a defense-in-depth issue. The affected behavior is reachable only when checkpoint bytes at rest in the backing store can be modified by an unauthorized party. In most deployments that prerequisite already implies a serious incident; the additional concern is turning "checkpoint-store write access" into code execution in the application runtime. This issue has been fixed in version 4.1.1.			
langflow-ai--langflow	A vulnerability was identified in langflow-ai langflow up to 1.9.3. This affects an unknown function of the component Bundle URL Loader. The manipulation leads to code injection. The attack needs to be performed locally. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	5.3	CVE-2026-12822
leejet--stable-diffusion.cpp	stable-diffusion.cpp is a pure C/C++ library for running diffusion model (Stable Diffusion, Flux, Wan, Qwen Image, Z-Image, and more) inference. Versions prior to master-584-0a7ae07 are vulnerable to an out-of-bounds reads error through PyTorch checkpoint pickle opcode parsing. The pickle .ckpt parser in src/model.cpp did not consistently check that enough input remained before reading opcode arguments or advancing the parser buffer with a crafted or truncated .ckpt file. Throughout the pickle parser, opcode handlers advanced the parser position with expressions such as buffer += N without first checking that buffer + N <= buffer_end. A truncated file could therefore cause reads past the end of the metadata buffer. LibFuzzer found crashes in under one second using malformed checkpoint inputs. Any application using affected stable-diffusion.cpp releases to load untrusted .ckpt model files could be vulnerable. The attack requires the victim or application to load a .ckpt file from an untrusted source, such as a downloaded model from a model sharing site. This issue has been fixed in version master-584-0a7ae07. If developers are unable to immediately update their applications, they can work around this issue by ensuring they do not load .ckpt checkpoint files from untrusted sources. They should prefer trusted model sources and safer formats such as .safetensors where possible.	2026-06-16	5.5	CVE-2026-47748
leethompson--Lazy Content Slider Plugin	WordPress Lazy Content Slider Plugin 3.4 contains a cross-site request forgery vulnerability that allows attackers to perform unauthorized actions by crafting malicious HTML forms. Attackers can trick authenticated administrators into submitting POST requests to the plugin settings page via lzcs_admin.php to modify plugin configuration parameters like lzcs_color and lzcs_count.	2026-06-15	4.3	CVE-2016-20074
legalweb--WP DSGVO Tools (GDPR)	The WP DSGVO Tools (GDPR) plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.1.39. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to supply an arbitrary victim email address and trigger immediate SAR processing via the process_now and is_ajax parameters, receiving tokenized download links (zip_link, pdf_link) in the HTTP response that expose the victim's personal data - including WordPress account details, comment author names, email addresses, IP addresses, and comment content - without any proof of ownership. The nonce used for the CSRF check is publicly	2026-06-19	5.3	CVE-2026-10034

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	rendered by the SAR shortcode form and is shared across all anonymous visitors, meaning any unauthenticated attacker can trivially obtain a valid nonce and bypass this gate entirely.			
lemonldap-ng--lemonldap-ng	A vulnerability was detected in lemonldap-ng up to 2.23.0. Impacted is an unknown function in the library lemonldap-ng-portal/lib/Lemonldap/NG/Portal/CDC.pm of the component SAML Common Domain Cookie Endpoint. Performing a manipulation of the argument url results in open redirect. The attack is possible to be carried out remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	4.3	CVE-2026-12804
libexpat project--libexpat	In libexpat before 2.8.2, there is a heap-based buffer overflow in doProlog in xmlparse.c because scaffold backing array reallocation is mishandled when there is data-structure sharing across parsers.	2026-06-19	6.9	CVE-2026-56132
libexpat project--libexpat	libexpat before 2.8.2 has an integer overflow in storeAtts.	2026-06-21	6.9	CVE-2026-56403
libexpat project--libexpat	libexpat before 2.8.2 has an integer overflow in addBinding.	2026-06-21	6.9	CVE-2026-56404
libexpat project--libexpat	libexpat before 2.8.2 has an integer overflow in getAttributeld.	2026-06-21	6.9	CVE-2026-56405
libexpat project--libexpat	libexpat before 2.8.2 has an integer overflow in XML_ParseBuffer because it lacked a check that was present in XML_Parse.	2026-06-21	6.9	CVE-2026-56406
libexpat project--libexpat	libexpat before 2.8.2 has an integer overflow in doProlog that is related to storeEntityValue and entity textLen.	2026-06-21	6.9	CVE-2026-56407
libexpat project--libexpat	libexpat before 2.8.2 has an integer overflow in copyString.	2026-06-21	6.9	CVE-2026-56408
libexpat project--libexpat	xmlwf in libexpat before 2.8.2 has an integer overflow for the output filename when -d outputDir is used.	2026-06-21	6.5	CVE-2026-56409
libexpat project--libexpat	xmlwf in libexpat before 2.8.2 has an integer overflow in resolveSystemId.	2026-06-21	6.9	CVE-2026-56410
libexpat project--libexpat	xmlwf in libexpat before 2.8.2 has an integer overflow in endDoctypeDecl via NOTATION declarations.	2026-06-21	6.9	CVE-2026-56411
libexpat project--libexpat	libexpat before 2.8.2 lacks handler call depth tracking for calls to XML_ResumeParser from within handlers in cases of a policy violation. Thus, a use-after-free can occur (similar to the CVE-2026-50219 situation).	2026-06-19	4.9	CVE-2026-56131
libexpat project--libexpat	libexpat before 2.8.2 does not consider XML_TOK_DATA_CHARS in doCdataSection and thus lacks handler call depth tracking for various calls from within handlers in cases of a policy violation. Thus, a use-after-free can occur. NOTE: this issue exists because of an incomplete fix for CVE-2026-50219.	2026-06-21	4.9	CVE-2026-56412
libssh2--libssh2	libssh2 through 1.11.1, fixed in commit 2dae302, contains an out-of-bounds heap read vulnerability in the sftp_symlink() function in src/sftp.c that allows a malicious SSH server or man-in-the-middle attacker to disclose heap memory contents or cause a crash by sending a crafted SSH_FXP_NAME response. Attackers can supply a link_len value larger	2026-06-18	6.5	CVE-2025-15661

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	than the actual packet data in SSH_FXP_NAME responses for SFTP READLINK and REALPATH operations, triggering a heap buffer over-read of up to target_len minus one bytes due to the missing validation of available packet buffer size before the memcpy operation.			
libssh2--libssh2	libssh2 through 1.11.1, fixed in commit 1762685, contains a pre-authentication denial of service vulnerability in the SSH_MSG_EXT_INFO handler in src/packet.c that allows a malicious SSH server to cause a client CPU exhaustion loop by sending a crafted extension count value. A malicious server can set nr_extensions to 0xFFFFFFFF during key exchange, causing the client to spin in a tight CPU loop for over 60 seconds because return values from _libssh2_get_string() are unchecked and the session timeout does not apply to CPU-bound loops.	2026-06-17	5.9	CVE-2026-55199
Liquid Web / StellarWP--Event Tickets	Unauthenticated Bypass Vulnerability in Event Tickets <= 5.27.5 versions.	2026-06-15	6.5	CVE-2026-42662
liseperu--Elizaibots	Contributor Cross Site Scripting (XSS) in Elizaibots <= 1.0.2 versions.	2026-06-15	6.5	CVE-2025-15659
lsegal--yard	YARD is a documentation generation tool for the Ruby programming language. Prior to version 0.9.44, YARD's static cache lookup reads a request path before the router's path cleanup runs. When a server is configured with a document root, a traversal path such as `./../yard-cache-secret.html` is joined against that root and can return a readable sibling `.html` file outside the intended static tree. Version 0.9.44 patches the issue.	2026-06-19	5.3	CVE-2026-49342
Mamunur Rashid--Classified Listing	Unauthenticated Broken Access Control in Classified Listing <= 5.3.8 versions.	2026-06-15	6.5	CVE-2026-42640
Mamunur Rashid--Classified Listing	Subscriber Broken Access Control in Classified Listing <= 5.3.9 versions.	2026-06-15	6.3	CVE-2026-42651
marimo-team--marimo	marimo before 0.23.9 contains a reflected cross-site scripting vulnerability in the notebook page that allows unauthenticated attackers to inject arbitrary JavaScript by exploiting improper escaping of single quotes in the file query parameter reflected into an inline JavaScript string literal. Attackers can craft a malicious link with a payload beginning with __new__ to bypass the 404 check and inject JavaScript into the page, which executes without Content-Security-Policy restrictions in the origin of a victim's marimo server.	2026-06-17	6.1	CVE-2026-54386
markdown-it--markdown-it	markdown-it is a Markdown parser. Versions 14.1.1 and below contain a denial-of-service vulnerability when typographer: true is enabled, due to quadratic (O(n^2)) processing in the smartquotes rule. The issue stems from repeatedly modifying strings with replaceAt(), which performs O(n) slicing and concatenation per quote character. This can cause excessive CPU consumption when parsing quote-heavy, user-supplied markdown and may let attackers degrade or disrupt service availability. Although typographer is disabled by default, many production apps enable it for	2026-06-17	5.3	CVE-2026-48988

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	smart typography, making the issue relevant. This issue has been fixed in version 14.2.0.			
MarketingFire--Widget Options	Insertion of sensitive information into sent data vulnerability in MarketingFire Widget Options allows Retrieve Embedded Sensitive Data. This issue affects Widget Options: from n/a through 4.0.1.	2026-06-17	6.5	CVE-2024-35690
Mattermost--Mattermost	Mattermost Desktop App versions <=6.1 5.5.13.0 fail to restrict the allow list of domains to which NTLM credentials were forwarded to in the Mattermost Desktop App which allows any user on a server without the image proxy enabled to intercept other users credentials via embedding an image that routes to an external web server. Mattermost Advisory ID: MMSA-2026-00651	2026-06-15	6.3	CVE-2026-6517
Mattermost--Mattermost	Mattermost Desktop App versions <=6.1 5.5.13.0 fail to account for attempting to open extremely long URLs in the Mattermost Desktop App which allows a malicious server owner to crash the application via including a script to call window.open on a very large URL. Mattermost Advisory ID: MMSA-2026-00652	2026-06-15	6.5	CVE-2026-8683
mbis--Permalink Manager Lite	The Permalink Manager Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via post titles in the admin URI Editor interface in all versions up to, and including, 2.5.3.3 due to insufficient output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in the admin Permalink Manager page that will execute whenever an administrator accesses the Permalink Manager page.	2026-06-17	6.4	CVE-2026-8494
mcdope--pam_usb	pam_usb provides hardware authentication for Linux using removable media. In versions prior to 0.9.2, getenv() environment variables XRDP_SESSION, DISPLAY and TMUX allow environment variable injection into local-check logic. These environment variables influence whether a current session is local or remote, and a PAM module that runs in the context of setuid binaries (sudo, su), getenv() returns attacker-controlled values whenever the process environment has been manipulated by a local user. This issue has been fixed in version 0.9.2.	2026-06-18	6.3	CVE-2026-48980
mcdope--pam_usb	pam_usb provides hardware authentication for Linux using ordinary removable media. In versions prior to 0.9.2, pam_usb calls xmlReadFile() with flags=0 when loading the configuration file, allowing libxml2 to process external entity references (XXE), potentially making outbound network connections or local file reads at XML parse time from the context of the authenticating process. The vulnerability requires the configuration file to contain crafted XML entity references. Since pam_usb.conf is root-owned, direct exploitation requires prior write access to the config, but the defence-in-depth impact is significant given that pam_usb.so runs in setuid contexts (sudo, su). This issue has been fixed in version 0.9.2.	2026-06-18	6.7	CVE-2026-48981
mcdope--pam_usb	pam_usb provides hardware authentication for Linux using ordinary removable media. In versions prior to 0.9.2, when updating a one-time pad file, a temporary file is created using open() without the O_EXCL flag. Without O_EXCL, the create operation is not atomic: two concurrent processes racing to update the same pad may both succeed in opening the file, with the second write silently overwriting the first. The one-time pad is the core replay-prevention mechanism of pam_usb. A successful race could result in the stored pad value diverging from what either process	2026-06-18	5.8	CVE-2026-48982

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	expected, potentially causing authentication failures or, in a precisely timed attack, creating a window for pad reuse. This issue has been fixed in version 0.9.2.			
mcdope-- pam_usb	pam_usb provides hardware authentication for Linux using ordinary removable media. In versions prior to 0.9.2, a symlink race condition exists in per-device and per-user pad directory creation. pam_usb uses a check-then-act pattern: it calls lstat() to test for existence and then calls mkdir() separately to create the directory. A local attacker can win the race between these calls by replacing the target path with a symlink to a directory they control. If successful, one-time pad files may be written to an attacker-controlled location, potentially exposing future pad values before use or disrupting authentication. This issue has been fixed in version 0.9.2.	2026-06-18	5.8	CVE-2026-48983
mcdope-- pam_usb	pam_usb provides hardware authentication for Linux using ordinary removable media. In versions 0.9.1 and below, pusb_is_loginctl_local() can cause a NULL dereference crash when parsing loginctl output. The function calls popen() and reads the result; if the Remote field is only a newline, fgets() succeeds but strtok_r(buf, "\n", &saveptr) returns NULL. A subsequent strcmp(is_remote, "no") then dereferences NULL, causing undefined behavior (typically SIGSEGV) and crashing the PAM module. This can crash the authenticating process (e.g., sudo, login) and, depending on PAM stack configuration, deny access for all users of the affected service. This issue has been fixed in version 0.9.2.	2026-06-18	5.5	CVE-2026-48985
mcdope-- pam_usb	pam_usb provides hardware authentication for Linux using ordinary removable media. In versions 0.9.1 and below, the xfree() memory release helper in calls free() without first zeroing the buffer contents, releasing heap-allocated buffers containing sensitive data - including one-time pad bytes read from disk - without clearing, leaving the sensitive content in freed heap memory until it happens to be overwritten by a subsequent allocation. On a system where a use-after-free condition exists, or where a heap inspection primitive becomes available, this could allow recovery of pad values or other authentication material from freed memory regions. This is a defence-in-depth requirement consistent with prior hardening work in this codebase (GHSA-vx6f-rrqr-j87c applied explicit_bzero to some pad paths; this issue generalises the pattern to the central deallocation helper).	2026-06-18	4.7	CVE-2026-48984
mcdope-- pam_usb	pam_usb provides hardware authentication for Linux using removable media. In pam_usb 0.9.1 and earlier, usb_get_process_parent_id() can cause an infinite loop DoS because it does not initialize *ppid on failure. In pusb_local_login(), the same variable is reused as input and output in a process-tree while loop; if /proc/<pid>/stat cannot be read (for example, when an ancestor process exits during authentication), the PID is not updated and the loop does not terminate. This hangs the authenticating process (such as sudo, sshd, or login) until it is forcibly terminated. This issue has been fixed in version 0.9.2.	2026-06-18	4.7	CVE-2026-48986
medkey-org-- medkey	A security flaw has been discovered in medkey-org medkey up to fc09b7ba9441ff590b72d428d5380834216b09ed. Impacted is the function actionGetPatientById of the file app\modules\medical\port\rest\controllers\PatientController.php of the component HTTP REST API. The manipulation of the argument ID results in	2026-06-15	4.3	CVE-2026-12207

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	improper control of resource identifiers. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The vendor was contacted early about this disclosure but did not respond in any way.			
Microsoft--GitHub Copilot Chat	Initialization of a resource with an insecure default in GitHub Copilot and Visual Studio Code allows an unauthorized attacker to disclose information over a network.	2026-06-19	6.5	CVE-2026-50519
Microsoft--Microsoft 365 Copilot	Improper neutralization of special elements used in a command ('command injection') in Microsoft Copilot allows an unauthorized attacker to perform tampering over a network.	2026-06-19	6.5	CVE-2026-42895
mohammadtanzilurrahman--Static Block	The Static Block plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.2. This is due to the static_block_content() shortcode handler retrieving a post via get_post() using an attacker-supplied 'id' attribute and outputting its post_content without verifying the post's status (private, draft, pending) or the requesting user's capability to view it. This makes it possible for authenticated attackers, with contributor-level access and above, to read the contents of arbitrary posts, including private and draft static blocks (and any other post type) created by administrators, by embedding the [static_block_content id="X"] shortcode in their own content and previewing it.	2026-06-16	4.3	CVE-2026-10780
Mojoomla--School Management	Unauthenticated Insecure Direct Object References (IDOR) in School Management <= 93.1.0 versions.	2026-06-17	5.3	CVE-2025-15657
mojoomla--WPAMS	Subscriber Arbitrary Content Deletion in WPAMS < 49.5.3 versions.	2026-06-16	6.5	CVE-2026-39433
Montodel--House-Rental-Management	A flaw has been found in Montodel House-Rental-Management up to 90010017b81265eb1ef3810268909f7719a33863. This affects an unknown part of the file /index.php?page=houses. This manipulation of the argument ID causes sql injection. The attack is possible to be carried out remotely. The exploit has been published and may be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	6.3	CVE-2026-12776
mra13 / Team Tips and Tricks HQ--Stripe Payments	Unauthenticated Bypass Vulnerability in Stripe Payments <= 2.0.98 versions.	2026-06-15	6.5	CVE-2026-42752
multer--multer	Impact: multer versions 2.0.0-alpha.1 through 2.1.1 and 3.0.0-alpha.1 are vulnerable to a Denial of Service when using diskStorage. Aborted or malformed multipart uploads leave orphaned partial files on disk because the Readable.pipe() call does not propagate the stream destroy signal to the underlying fs.WriteStream. An attacker can exhaust disk space by triggering many aborted uploads, with no application bug required. Patches: Users should upgrade to multer 2.2.0 (2.x line) or 3.0.0-alpha.2	2026-06-15	5.3	CVE-2026-5038

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(3.x prerelease). Both versions track in-flight write streams and clean them up on the abort path. Workarounds: None.			
myCred--Bookify	Subscriber Broken Access Control in Bookify <= 1.1.1 versions.	2026-06-15	6.5	CVE-2025-69332
myCred--myCred	Subscriber Broken Access Control in myCred <= 3.0.3 versions.	2026-06-15	6.5	CVE-2026-40794
Nasir Ahmed--Advanced Form Integration	Subscriber Broken Access Control in Advanced Form Integration <= 1.126.12 versions.	2026-06-15	6.5	CVE-2026-42659
nesquena--hermes-webui	Hermes WebUI before 0.51.443 contains a broken access control vulnerability in the /api/session endpoint that allows authenticated users to disclose cross-profile session transcripts. Attackers can bypass profile boundary checks by directly querying session IDs belonging to other profiles via GET /api/session?session_id=<foreign_id>&messages=1 to retrieve unauthorized conversation transcripts and metadata.	2026-06-17	6.5	CVE-2026-55197
nesquena--hermes-webui	Hermes WebUI before 0.51.443 contains an authorization bypass vulnerability in the session export endpoint that allows authenticated users to access sessions from other profiles. The _handle_session_export handler in api/routes.py fails to verify active-profile ownership before serializing session data, enabling attackers to exfiltrate foreign session transcripts by guessing or knowing session identifiers.	2026-06-17	6.5	CVE-2026-55198
nesquena--hermes-webui	Hermes WebUI before 0.51.468 contains a resource exhaustion vulnerability in the unauthenticated POST /api/onboarding/oauth/start endpoint that allows unbounded accumulation of in-memory flow state and daemon threads. Attackers can send repeated or concurrent requests to exhaust server memory and thread resources, potentially triggering repeated outbound device-code requests to upstream OAuth providers.	2026-06-18	5.3	CVE-2026-55205
NI--grpc-device	There is an unchecked enum cast vulnerability in NI grpc-device BeginSidebandStream that may allow an attacker to trigger invalid enum states and undefined behavior, potentially resulting in a denial of service. Successful exploitation requires an attacker to supply a specially crafted message containing an out-of-range value. This affects NI grpc-device 2.17.0 and prior versions.	2026-06-19	6.5	CVE-2026-48140
NI--grpc-device	There is a memory leak in NI grpc-device BeginSidebandStream that may result in denial of service due to memory exhaustion. This affects NI grpc-device 2.17.0 and prior versions.	2026-06-19	5.3	CVE-2026-48141
nilfs-dev--nilfs-utils	NILFS utilities through 2.3.0, fixed in commit 26efb5d, nilfs_sb_is_valid() function fails to validate s_log_block_size field in NILFS2 superblock before bit-shift operations. Attackers supplying crafted NILFS2 images trigger undefined behavior through oversized shifts or out-of-memory conditions, crashing tools like nilfs-tune and dumpseg.	2026-06-18	5.5	CVE-2026-55392
NousResearch--hermes-agent	Hermes Agent before 0.16.0 creates response_store.db and webhook_subscriptions.json with world-readable permissions (mode 0o644), exposing conversation history and HMAC secrets to local users. Attackers with local filesystem access can read these files directly to obtain	2026-06-17	5.5	CVE-2026-53870

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sensitive data including conversation history, tool payloads, prompts, and per-route HMAC secrets.			
OceanWP-- Ocean Product Sharing	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in OceanWP Ocean Product Sharing allows Stored XSS. This issue affects Ocean Product Sharing: from n/a through 2.2.2.	2026-06-18	5.9	CVE-2026-56007
OFFIS--DCMTK	A flaw has been found in OFFIS DCMTK up to 3.7.0. The affected element is the function XMLNode::parseFile in the library ofstd/libsrc/ofxml.cc. Executing a manipulation can lead to heap-based buffer overflow. The attack may be performed from remote. The exploit has been published and may be used. This patch is called 1d4b3815c0987840a983160bfc671fef63a3105b. It is best practice to apply a patch to resolve this issue. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	2026-06-21	6.3	CVE-2026-12805
ollybach-- WPPizza	Subscriber Sensitive Data Exposure in WPPizza <= 3.19.9 versions.	2026-06-15	6.5	CVE-2026-40796
OpenBSD-- OpenBSD	sppp_pap_input in sys/net/if_spppsubr.c in OpenBSD before 076e2b1 allows authentication bypass via certain zero values for lengths.	2026-06-17	5.8	CVE-2026-55706
openbsd--src	OpenBSD before commit 6a23123 (2026-06-18) contains an out-of-bounds read vulnerability in the mpl_s_do_error function within sys/netmpls/mpls_input.c that allows remote attackers to disclose kernel stack memory by sending crafted MPLS frames with 16 labels and no Bottom-of-Stack bit set.	2026-06-18	5.3	CVE-2026-56099
OpenClaw-- OpenClaw	OpenClaw before 2026.5.12 contains a cross-site scripting vulnerability in exported session HTML that preserves unsafe javascript: and data: links in generated content. Attackers can execute browser-side scripts if a trusted operator opens the exported file and activates a malicious link.	2026-06-16	6.1	CVE-2026-53841
OpenClaw-- OpenClaw	OpenClaw before 2026.4.29 contains a session visibility check bypass vulnerability in shared memory search that allows authenticated callers to access memory entries without proper authorization. Attackers can skip session visibility guards on the search path to retrieve memory entries that should not be visible to their session.	2026-06-16	6.5	CVE-2026-53844
OpenClaw-- OpenClaw	OpenClaw before 2026.4.25 contains a privilege escalation vulnerability in internal and webchat command authentication that allows senders to inherit wildcard ownerAllowFrom state across channel boundaries. Attackers can exploit this by sending commands on affected internal or webchat paths to execute owner-style command behavior outside intended channel scope, potentially bypassing access controls.	2026-06-16	6.5	CVE-2026-53854
OpenClaw-- OpenClaw	OpenClaw before 2026.5.26 contains a hostname validation vulnerability allowing attackers to bypass blocklist comparisons using trailing-dot notation in model or workspace-derived URLs. Attackers can exploit inconsistent hostname checks to reach destinations that operators intended to block through hostname policies.	2026-06-16	6.5	CVE-2026-53859
OpenClaw-- OpenClaw	OpenClaw before 2026.5.6 contains an allowlist bypass vulnerability in the macOS Swift exec feature that misses combined POSIX inline-command flags. Attackers can execute shell content outside the intended allowlist	2026-06-16	6.6	CVE-2026-53861

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	check by using combined flag forms, potentially allowing unauthorized command execution depending on operator configuration.			
OpenClaw-- OpenClaw	OpenClaw before 2026.5.6 contains a privilege escalation vulnerability in the Active Memory write scope that allows Gateway operators with operator.write access to modify global configuration without requiring operator.admin privileges. Attackers with operator.write access can exploit insufficient scope validation to apply unauthorized configuration changes beyond the intended write scope.	2026-06-16	5.4	CVE-2026-53847
OpenClaw-- OpenClaw	OpenClaw before 2026.4.25 contains a control scope enforcement bypass vulnerability in the focus command that allows authenticated callers to execute the command without proper authorization checks. Attackers can trigger the focus command to change focus state outside intended caller authority, potentially enabling unauthorized operations depending on gateway configuration and input trust levels.	2026-06-16	5.5	CVE-2026-53850
OpenClaw-- OpenClaw	OpenClaw before 2026.5.12 contains a notification bypass vulnerability allowing Slack reaction events to enter the agent pipeline despite disabled reaction notifications. Attackers can trigger unintended agent processing by sending reaction events when the feature is enabled, potentially leading to unauthorized processing of lower-trust input.	2026-06-16	5.3	CVE-2026-53851
OpenClaw-- OpenClaw	OpenClaw before 2026.4.25 contains a scope containment bypass vulnerability in device re-pairing that allows authenticated operators to restore broader scopes than intended by submitting empty-scope re-pairing requests. Attackers can exploit this by sending re-pairing requests with empty scope sets to skip containment guards and retain unauthorized device access.	2026-06-16	5.4	CVE-2026-53852
OpenClaw-- OpenClaw	OpenClaw 2026.4.23 before 2026.4.24 contains an insecure file permissions vulnerability in config recovery that restores OpenClaw.json with overly broad permissions. Local attackers on shared hosts can read sensitive configuration data by exploiting the recovery path to access the restored config file.	2026-06-16	5.5	CVE-2026-53856
OpenClaw-- OpenClaw	OpenClaw before 2026.5.6 contains a hook bypass vulnerability where skill commands routed through the affected dispatch path skip before-tool-call hook coverage. Attackers can exploit this by sending skill commands through the vulnerable dispatch path to bypass hook-based auditing and policy enforcement mechanisms.	2026-06-16	4.3	CVE-2026-53845
OpenClaw-- OpenClaw	OpenClaw before 2026.5.26 contains an exec allowlist bypass vulnerability allowing authenticated operators to execute wrapper-level side effects outside allowlisted command intent. Attackers can craft command requests that bypass allowlist validation by leveraging transparent command wrappers to perform unintended operations.	2026-06-16	4.3	CVE-2026-53848
OpenClaw-- OpenClaw	OpenClaw before 2026.5.7 contains a sender policy bypass vulnerability in BlueBubbles that allows participants to match allowlist entries through conversation metadata rather than stable sender identity. Attackers can influence conversation-level identifiers to receive agent responses intended for configured senders, potentially bypassing access controls.	2026-06-16	4.2	CVE-2026-53860
OpenClaw-- OpenClaw	OpenClaw before 2026.5.12 contains a bootstrap token replay vulnerability allowing callers with pending token access to reuse tokens	2026-06-16	4.2	CVE-2026-53862

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	with broader requested scopes. Attackers can replay bootstrap tokens before approval to escalate pairing authority beyond intended scope limits.			
OpenStack--Horizon	OpenStack Horizon before 25.7.4 produces scripts for OpenStack RC file downloading that may have a crafted project name with shell metacharacters. NOTE: some parties consider this a security hardening opportunity to address certain types of user error, not a vulnerability.	2026-06-17	6	CVE-2026-55748
OpenStack--Nova	In OpenStack Nova before 33.0.2, the server create API does not strip certain hint data. The resulting instance has no Placement allocation.	2026-06-16	5.4	CVE-2026-46448
OPMC--WooCommerce Anti-Fraud	Unauthenticated Broken Access Control in WooCommerce Anti-Fraud <= 7.2.6 versions.	2026-06-17	6.5	CVE-2026-49072
OPMC--WooCommerce Dropshipping	Unauthenticated Broken Authentication in WooCommerce Dropshipping <= 5.2.4 versions.	2026-06-17	6.5	CVE-2026-49071
optimole--Optimole Optimize Images Convert WebP & AVIF CDN & Lazy Load Image Optimization	The Optimole - Optimize Images Convert WebP & AVIF CDN & Lazy Load Image Optimization plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.2.6. This is due to missing or incorrect nonce validation on the replace_file function. This makes it possible for unauthenticated attackers to overwrite existing media attachments with attacker-supplied file content by supplying a forged multipart POST request targeting any attachment the victim has edit_post capability over via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. The forged request requires a victim with at least Author-level privileges, as the handler enforces a current_user_can('edit_post', \$id) check; tricking an Author-level or higher user into clicking a crafted link is sufficient to trigger the overwrite against attachments that user can edit.	2026-06-18	4.3	CVE-2026-11784
Oracle Corporation--Identity Manager	Vulnerability in the Identity Manager product of Oracle Fusion Middleware (component: End User Self Service). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Identity Manager. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Identity Manager accessible data as well as unauthorized read access to a subset of Identity Manager accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2026-06-16	6.5	CVE-2026-46810
Oracle Corporation--MySQL Shell	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell: Dump and Load). Supported versions that are affected are 8.4.0-8.4.9 and 9.0.0-9.7.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Shell. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Shell accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N).	2026-06-16	6.5	CVE-2026-46869

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation--MySQL Shell	Vulnerability in the MySQL Shell product of Oracle MySQL (component: Shell for VS Code). The supported version that is affected is 2026.2.0+9.6.1. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Shell. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Shell accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2026-06-16	6.5	CVE-2026-46871
Oracle Corporation--Oracle Access Manager	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Access Manager accessible data as well as unauthorized read access to a subset of Oracle Access Manager accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2026-06-16	6.5	CVE-2026-35261
Oracle Corporation--Oracle Access Manager	Vulnerability in the Oracle Access Manager product of Oracle Fusion Middleware (component: Authentication Engine). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Access Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Access Manager, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Access Manager accessible data as well as unauthorized read access to a subset of Oracle Access Manager accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-06-16	6.1	CVE-2026-46812
Oracle Corporation--Oracle Application Development Framework (ADF)	Vulnerability in the Oracle Application Development Framework (ADF) product of Oracle Fusion Middleware (component: Security Framework). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Development Framework (ADF). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Development Framework (ADF), attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Development Framework (ADF) accessible data as well as unauthorized read access to a subset of Oracle Application Development Framework (ADF) accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2026-06-16	6.1	CVE-2026-46770
Oracle Corporation--Oracle Application Development	Vulnerability in the Oracle Application Development Framework (ADF) product of Oracle Fusion Middleware (component: Java Business Objects). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Application Development Framework (ADF)	2026-06-16	4.1	CVE-2026-46771

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Framework (ADF)	executes to compromise Oracle Application Development Framework (ADF). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Application Development Framework (ADF) accessible data. CVSS 3.1 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).			
Oracle Corporation-- Oracle Application Development Framework (ADF)	Vulnerability in the Oracle Application Development Framework (ADF) product of Oracle Fusion Middleware (component: ADF Faces). Supported versions that are affected are 12.2.1.4.0 and 14.1.2.0.0. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Application Development Framework (ADF) executes to compromise Oracle Application Development Framework (ADF). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Application Development Framework (ADF) accessible data as well as unauthorized update, insert or delete access to some of Oracle Application Development Framework (ADF) accessible data. CVSS 3.1 Base Score 4.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:N).	2026-06-16	4.7	CVE-2026-46772
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: VMSVGA device). The supported version that is affected is 7.2.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.0 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).	2026-06-16	6	CVE-2026-46768
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: VMSVGA device). The supported version that is affected is 7.2.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N).	2026-06-16	6	CVE-2026-46825
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: VMSVGA device). The supported version that is affected is 7.2.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	2026-06-16	6	CVE-2026-46877

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle WebCenter Content	Vulnerability in the Oracle WebCenter Content product of Oracle Fusion Middleware (component: Content Server). The supported version that is affected is 14.1.2.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Content. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebCenter Content accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2026-06-16	5.3	CVE-2026-46790
Oracle Corporation-- PeopleSoft Enterprise CS Campus Community	Vulnerability in the PeopleSoft Enterprise CS Campus Community product of Oracle PeopleSoft (component: Integration and Interfaces). The supported version that is affected is 9.2.38. Easily exploitable vulnerability allows high privileged attacker with network access via HTTPS to compromise PeopleSoft Enterprise CS Campus Community. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise CS Campus Community accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise CS Campus Community accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N).	2026-06-16	6.5	CVE-2026-46979
Oracle Corporation-- WebLogic Server	Vulnerability in the WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 14.1.2.0.0 and 15.1.1.0.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise WebLogic Server. Successful attacks of this vulnerability can result in takeover of WebLogic Server. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).	2026-06-16	6.6	CVE-2026-35291
pgadmin.org-- pgAdmin 4	Open redirect in pgAdmin 4's multi-factor authentication flow. The MFA validate and register endpoints honoured the user-supplied 'next' query/form parameter without confirming the target pointed back inside pgAdmin, so an authenticated victim who clicked /mfa/validate?next=<external> -- a link typically delivered by phishing -- would be sent to an attacker-controlled host directly out of the trusted auth flow. The defect is a trusted-domain redirect, not a privilege bypass: the attacker gains no read/write access to pgAdmin or the victim's database, but the redirect launders the attacker's destination through pgAdmin's URL, which raises the success rate of credential-phishing follow-on against the victim. Fix introduces a same-origin_is_safe_redirect_url helper and gates every MFA redirect that consumes user-supplied 'next' values through it. The helper allows only relative paths and absolute URLs whose scheme is http(s) and whose host matches the current request host; it rejects external hosts in absolute and protocol-relative form, non-http schemes (javascript:, data:, mailto:), userinfo tricks (http://localhost@attacker/), and backslash variants that some browsers normalize to forward slashes. Unsafe targets fall back to the internal browser index. A dedicated regression test exercises each accept/reject category and the original reporter PoC. This issue affects pgAdmin 4: from 6.0 before 9.16.	2026-06-18	4.3	CVE-2026-12049
pgadmin.org-- pgAdmin 4	SQL injection in pgAdmin 4's named restore point endpoint (POST /browser/server/restore_point/{gid}/{sid}). The user-supplied 'value' field was interpolated directly into the SQL string with str.format() instead of being passed as a bound parameter, allowing an authenticated pgAdmin	2026-06-18	4.3	CVE-2026-12050

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	user with a connected PostgreSQL session to inject additional statements through that endpoint. The injected SQL executes under the database role the user is already authenticated as. The defect does not cross a privilege boundary -- the user already has direct SQL access to that role through the Query Tool -- so the attacker gains no capability beyond what their database role already grants them. The marginal impact accounts for the fact that the injection path is not the documented SQL-execution interface, so a deployment that gates the Query Tool at the application layer could see SQL executed through a path it did not anticipate. Fix passes the restore point name as a bound parameter and schema-qualifies the function call as pg_catalog.pg_create_restore_point so a non-default search_path on the connection cannot redirect the call to a shadow definition. A regression test asserts the value arrives as a bound parameter and not spliced into the SQL string. This issue affects pgAdmin 4: from 1.0 before 9.16.			
phppoet-- SysBasics Customize My Account for WooCommerce Dashboard, Endpoints, Avatar & Menu Manager	The Customize My Account For Woocommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'sysbasics_user_avatar' shortcode in versions up to, and including, 4.3.6. This is due to insufficient input sanitization and output escaping on user supplied attributes (min_height, min_width, max_height, max_width) in the wcmamtx_get_avatar_default() function, which are concatenated unescaped into the get_avatar() extra_attr style attribute. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-18	6.4	CVE-2026-12136
phppoet-- SysBasics Customize My Account for WooCommerce Dashboard, Endpoints, Avatar & Menu Manager	The SysBasics Customize My Account for WooCommerce - Dashboard, Endpoints, Avatar & Menu Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 4.3.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. Because the vulnerable plugin_options_page() function is only rendered within the WordPress admin dashboard, successful exploitation requires the targeted victim to be logged in with Shop Manager-level access or higher.	2026-06-18	6.1	CVE-2026-12137
picklescan-- picklescan	picklescan before 1.0.1 contains an unsafe pickle deserialization vulnerability allowing unauthenticated attackers to create arbitrary zero-byte files via logging.FileHandler class instantiation. Attackers can exploit this by crafting malicious pickle payloads to bypass RCE blocklists and create lock files or other filesystem artifacts, potentially causing denial of service or application disruption.	2026-06-20	6.5	CVE-2026-56304
pontedilana-- php-weasyprint	PhpWeasyPrint is a PHP library allowing PDF generation from a URL or an HTML page. Prior to version 2.6.0, `pontedilana/php-weasyprint` fetches the content of option values server-side via `file_get_contents()` when the value looks like a URL, without restricting the URL scheme. The `attachment` option of `Pdf` is the reachable sink: any value that passes `isOptionUrl()` (`filter_var(..., FILTER_VALIDATE_URL)`) is downloaded by the PHP process and embedded into the generated PDF. Because `FILTER_VALIDATE_URL` accepts `http`, `https`, `ftp`, `file` and PHP stream wrappers such as `php://`, an attacker who can influence the `attachment` value reaches both a **Server-Side Request Forgery** primitive (e.g.	2026-06-19	6.5	CVE-2026-49359

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	internal HTTP endpoints, cloud metadata) and a local file disclosure primitive (`file://`, `php://filter/...`), with the fetched bytes exfiltrated as a PDF attachment. This is the same class of issue KnPLabs/snappy patched for its `xsl-style-sheet` option in GHSA-c5fp-p67m-gq56. The library is documented as a one-to-one substitute for KnPLabs/snappy and shares the same code shape. PhpWeasyPrint version 2.6.0 contains a patch for the issue.			
PraisonAI-- PraisonAI	PraisonAI before 1.5.115 contains an information disclosure vulnerability in the MultiAgentLedger component that allows attackers to access sensitive data by registering agents with duplicate IDs. Attackers can exploit the lack of agent ID uniqueness enforcement to share ledger instances and expose system prompts and conversation history between agents.	2026-06-18	6.5	CVE-2026-56077
PraisonAI-- PraisonAI	PraisonAI before 1.5.128 caches tool approval decisions by tool name only, not by invocation arguments, allowing subsequent execute_command calls to bypass approval prompts. Attackers can exploit this by obtaining initial approval for a benign command, then silently exfiltrate API keys and credentials via subsequent shell commands without user consent.	2026-06-18	5.5	CVE-2026-56074
pressprimer-- PressPrimer Quiz AI Quiz Maker, Exam Builder & LMS Assessment Plugin	The PressPrimer Quiz - AI Quiz Maker, Exam Builder & LMS Assessment Plugin plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.3.0 via the 'rule_id' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with custom-level access and above, to modify or delete quiz rules belonging to other teachers, resulting in unauthorized tampering of another user's quiz structure.	2026-06-18	4.3	CVE-2026-10623
properfraction-- ProfilePress	Subscriber Cross Site Scripting (XSS) in ProfilePress <= 4.16.13 versions.	2026-06-15	6.5	CVE-2026-41556
purethemes-- WorkScout-Core	Unauthenticated Arbitrary File Deletion in WorkScout-Core <= 1.7.11 versions.	2026-06-17	6.5	CVE-2026-52716
pydantic-- pydantic-ai	Pydantic AI is a Python agent framework for building applications and workflows with Generative AI. In versions 1.56.0 through 1.101.0, 2.0.0b1, and 2.0.0b2, the cloud-metadata blocklist could be bypassed by encoding the metadata IP in an IPv6 transition form that the previous fix, CVE-2026-46678, did not decode, exposing cloud IAM short-term credentials. The previous remediation decoded only IPv4-mapped IPv6, 6to4, and the NAT64 well-known prefix, so the metadata guarantee did not hold for the remaining transition forms: IPv4-compatible IPv6 (::a.b.c.d), the NAT64 RFC 8215 local-use prefix (64:ff9b:1::/48), operator-chosen NAT64 prefixes, and ISATAP. The IPv6 wrapper is then delivered to the underlying IPv4 metadata endpoint. This occurs when an application using Pydantic AI opts a URL into force_download='allow-local' (which disables the default block on private/internal IPs) and runs on a network that actually routes the affected IPv6 transition forms: NAT64-configured networks (IPv6-only or dual-stack-with-NAT64 deployments, including some Kubernetes setups) for the NAT64 variants, or networks with an ISATAP tunnel for ISATAP. A standard dual-stack cloud VM or container does not route these forms and is not affected in practice. The IPv4-compatible and Teredo variants are deprecated and addressed as defense-in-depth. This is an	2026-06-16	6.8	CVE-2026-48782

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	incomplete fix of GHSA-cqp8-fcvh-x7r3 / CVE-2026-46678 (itself a follow-up to CVE-2026-25580). This issue has been fixed in version 2.0.0b3.			
Rain-Task Ltd.-- WPBakery Page Builder	Subscriber Broken Access Control in WPBakery Page Builder <= 8.7.2 versions.	2026-06-17	6.5	CVE-2026-45436
Rank Math SEO-- Rank Math SEO	Subscriber Broken Access Control in Rank Math SEO <= 1.0.271 versions.	2026-06-15	6.5	CVE-2026-34892
Rara Themes-- Metro Magazine	Missing Authorization vulnerability in Rara Themes Metro Magazine allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Metro Magazine: from n/a through 1.4.1.	2026-06-16	6.5	CVE-2026-40809
Rara Themes-- Metro Magazine	Missing Authorization vulnerability in Rara Themes Metro Magazine allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Metro Magazine: from n/a through 1.3.7.	2026-06-17	4.3	CVE-2024-37496
Really Simple Plugins B.V.-- Really Simple SSL	Subscriber Broken Access Control in Really Simple SSL <= 9.5.9 versions.	2026-06-15	6.5	CVE-2026-48969
Red Hat--Red Hat AI Inference Server	A flaw was found in vLLM, an open-source library for large language model inference. This vulnerability arises from improper handling of image metadata, specifically EXIF orientation and PNG transparency (tRNS) data, during image processing. When images are converted to RGB, transparency information may be implicitly discarded or remapped, leading to unexpected rendering of transparent pixels and distortion of input content. This can result in the model misinterpreting image content, potentially affecting the integrity of processed data.	2026-06-17	4.8	CVE-2026-12491
Red Hat--Red Hat Ansible Automation Platform 2	A flaw was found in the AWX GitHub webhook integration. When processing GitHub pull_request webhooks, the controller stores the pull_request.statuses_url value from the webhook payload without validating that it points to a trusted GitHub API endpoint. If a job template is configured with a GitHub Personal Access Token as its webhook credential, the controller later POSTs that token to the stored callback URL when posting job status updates. An attacker who can submit a correctly signed forged webhook using the job template's webhook_key can redirect the callback to an attacker-controlled URL and exfiltrate the configured GitHub PAT.	2026-06-19	6.3	CVE-2026-12726
Red Hat--Red Hat Ansible Automation Platform 2.7	A flaw was found in Ansible Lightspeed. This vulnerability, related to insufficient session expiration, allows a remote attacker to maintain persistent access to the Ansible Lightspeed instance. If an attacker exfiltrates a valid OAuth (Open Authorization) access token before a user logs out, they can continue to authenticate and access sensitive data. This is because the application fails to invalidate the token on the backend, leaving it valid until its natural expiration. This can lead to unauthorized read access to Ansible resources such as inventories, playbooks, and configuration data.	2026-06-15	5.3	CVE-2026-44188
Red Hat--Red Hat Directory Server 11	A flaw was found in 389 Directory Server. During schema reload, the attr_syntax_swap_ht() function unconditionally frees attribute syntax information nodes, bypassing the refcount-based deferred deletion used elsewhere in the attribute syntax subsystem. If an administrator triggers	2026-06-18	5	CVE-2026-11791

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	schema reload while concurrent LDAP query traffic is active, worker threads may access freed memory, resulting in use-after-free or double-free and a denial of service (server crash).			
Red Hat--Red Hat Directory Server 11	A flaw was found in 389 Directory Server in the <code>__aclp__normalize_acltxt()</code> function of <code>acldump.c</code> . A malformed ACL (Access Control Instruction) string can trigger heap-buffer-overflow writes and reads during ACL parsing. The function fails to validate that the ACL keyword has sufficient length after whitespace stripping, leading to a 1-byte out-of-bounds write and subsequent out-of-bounds reads. An authenticated user with write access to the <code>aci</code> attribute could send a crafted ACL value to silently corrupt heap memory in the directory server process.	2026-06-17	5.4	CVE-2026-12528
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in GnuTLS. The <code>`gnutls_pkcs11_token_set_pin`</code> function, used for changing the Security Officer PIN, can lead to a use-after-free vulnerability. This occurs when an attacker attempts to change the PIN with a NULL old PIN for a token that lacks a protected authentication path.	2026-06-16	6.6	CVE-2026-42014
Red Hat--Red Hat Enterprise Linux 10	A denial of service vulnerability was found in GStreamer's AV1 codec parser in <code>gst-plugins-bad</code> . The <code>gst_av1_parser_parse_tile_list_obu()</code> function passes a byte count to a bit-reader API that expects a bit count, causing parser desynchronization. A remote attacker could trick a user into opening a specially crafted AV1 media file, triggering an assertion abort and causing the application to crash.	2026-06-15	6.5	CVE-2026-52718
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in GNOME localsearch (previously known as tracker-miners) MP3 Extractor. When processing specially crafted MP3 files containing ID3v2.4 tags, a missing bounds check in the <code>`extract_performers_tags`</code> function can lead to a heap buffer overflow. This vulnerability allows a remote attacker to cause a Denial of Service (DoS) by triggering a read of unmapped memory. In some cases, it could also lead to information disclosure by reading visible heap data.	2026-06-16	5.6	CVE-2026-1764
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in the <code>`tracker-extract-mp3`</code> component of GNOME localsearch (previously known as tracker-miners). This vulnerability, a heap buffer overflow, occurs when processing specially crafted MP3 files. A remote attacker could exploit this by providing a malicious MP3 file, leading to a Denial of Service (DoS) where the application crashes. It may also potentially expose sensitive information from the system's memory.	2026-06-16	5.6	CVE-2026-1765
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in GNOME localsearch (previously known as tracker-miners) MP3 Extractor, specifically within the <code>tracker-extract-mp3</code> component. This heap buffer overflow vulnerability occurs when processing specially crafted MP3 files containing malformed ID3v2.3 COMM (Comment) tags. An attacker could exploit this by providing a malicious MP3 file, leading to a denial of service (DoS), which causes an application crash, and potentially disclosing sensitive information from the heap memory.	2026-06-16	5.6	CVE-2026-1766
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in the GNOME localsearch (previously known as tracker-miners) MP3 Extractor <code>`tracker-extract-mp3`</code> component. A remote attacker could exploit this heap buffer overflow vulnerability by providing a specially crafted MP3 file containing malformed ID3 tags. This incorrect length calculation during the parsing of performer tags can lead to a read	2026-06-16	5.6	CVE-2026-1767

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	beyond the allocated buffer, potentially causing a Denial of Service (DoS) due to a crash or enabling information disclosure.			
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in libXpm. A local user with low privileges could exploit an Out-of-Bounds Read vulnerability in the `xpmNextWord()` function by processing a specially crafted or very small XPM (X PixMap) image file. This improper validation of file boundaries can cause an internal pointer to read beyond the file's end, leading to application crashes and Denial of Service conditions.	2026-06-16	5.5	CVE-2026-4367
Red Hat--Red Hat Enterprise Linux 10	Multiple out-of-bounds read vulnerabilities were found in GStreamer's pcapparse element. Malformed PCAP records can trigger reads beyond buffer boundaries during IPv4/TCP header parsing. This element is primarily used in debugging pipelines, limiting real-world exposure. A local attacker could trick a user into processing a specially crafted PCAP file, potentially leading to a crash or information disclosure.	2026-06-15	5.3	CVE-2026-52721
Red Hat--Red Hat Enterprise Linux AI (RHEL AI) 3	A use-after-free vulnerability was found in FFmpeg's RASC video decoder. The decode_move() function initializes a read pointer into a decompressed buffer, but a subsequent reallocation of that same buffer during move-table processing leaves the pointer dangling. An attacker could exploit this by providing a specially crafted AVI file containing a malicious RASC video stream. When a user opens or plays the file, the decoder reads from freed heap memory, which could lead to a denial of service (crash).	2026-06-19	6.5	CVE-2026-12706
Red Hat--Red Hat Hardened Images	A flaw was found in Katello's of Red Hat Satellite. A content upload functionality where insufficient authorization checks in the ContentUploadsController allowed users with the edit_products permission to query content information for repositories outside the products they were authorized to manage. An authenticated attacker could exploit this issue to determine whether specific content exists within repositories that should otherwise be inaccessible. This issue does not allow unauthorized modification, import, or publication of content.	2026-06-17	4.3	CVE-2026-12515
RelyWP--Simple Cloudflare Turnstile	Unauthenticated Broken Authentication in Simple Cloudflare Turnstile <= 1.38.0 versions.	2026-06-15	5.8	CVE-2026-40799
rewish--WP Emmet	Administrator Cross Site Scripting (XSS) in WP Emmet <= 0.3.4 versions.	2026-06-15	5.9	CVE-2025-15658
rocklobsterinc--Bogo	The Bogo plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.9.1 via the bogo_rest_create_post_translation. This makes it possible for authenticated attackers, with subscriber-level access and above, to extract the raw title, content, excerpt, and password of any private, draft, or password-protected post by triggering its duplication via the translation endpoint and reading the returned title.raw, content.raw, and excerpt.raw fields of the duplicated post. This vulnerability is exploitable against posts written in a non-default locale, as authenticated subscribers can request a translation into the site's default locale to pass the locale-only permission gate. While subscribers can trigger the endpoint, this is only impactful at the Contributor-level as they can actually read the duplicated content.	2026-06-19	4.3	CVE-2026-9013

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rometheme--RTMKit	The RTMKit plugin for WordPress is vulnerable to Incorrect Authorization in all versions up to, and including, 2.0.7 This is due to the get_submission_content AJAX endpoint lacking a capability check to verify that a user has permission to access the requested form submission data. This makes it possible for authenticated attackers, with Contributor-level access and above, to view arbitrary form submissions from other users by iterating the entries_id parameter.	2026-06-16	6.5	CVE-2026-5149
rtCamp Inc.--rtMedia for WordPress, BuddyPress and bbPress	Subscriber Broken Access Control in rtMedia for WordPress, BuddyPress and bbPress <= 4.7.9 versions.	2026-06-15	6.5	CVE-2026-40773
RubyLouvre--avalon	A security vulnerability has been detected in RubyLouvre avalon up to 2.2.10. The impacted element is an unknown function of the file src/filters/index.js of the component Template Filter Handler. Such manipulation leads to improperly controlled modification of object prototype attributes. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	5.3	CVE-2026-12209
runtipi--runtipi	Runtipi is a personal homeserver orchestrator. In versions 4.9.1 through 4.9.3, Runtipi serves marketplace app logos from files inside cloned app-store repositories through an unauthenticated endpoint, which leads to arbitrary file read through app-store logo symlinks. The path guard checks only the lexical path before Node reads the file, so a Git app store that contains metadata/logo.jpg as a symbolic link can cause Runtipi to read and return the symlink target. Because the endpoint is public and the symlink target may point outside the cloned repository, this can expose local files from the Runtipi container such as /data/.env, /data/state/seed, logs, or application files. This can disclose JWT secrets, service credentials, local configuration, and operational logs depending on the instance. The issue has been fixed in version 4.10.0.	2026-06-16	6.5	CVE-2026-47277
Saad Iqbal--WP EasyPay	Cross-Site Request Forgery (CSRF) vulnerability in Saad Iqbal WP EasyPay allows Cross Site Request Forgery. This issue affects WP EasyPay: from n/a through 4.4.0.	2026-06-18	6.5	CVE-2026-56024
saadiqbal--Points Management System For Gamification, Ranks, Badges, and Loyalty Rewards Program myCred	The Points Management System For Gamification, Ranks, Badges, and Loyalty Rewards Program - myCred plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'wrap' Shortcode Attribute in all versions up to, and including, 3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-17	6.4	CVE-2026-8607
sc Internet Vivoo--WpStream	Subscriber Arbitrary File Upload in WpStream < 4.11.2 versions.	2026-06-15	5.4	CVE-2026-39527
shaarli--Shaarli	Shaarli is a personal bookmarking service. Versions 0.16.1 and prior contain a DOM-based Cross-Site Scripting (XSS) vulnerability in the Thumbnail Synchronizer feature. When an administrator runs the thumbnail update process, malicious bookmark titles are returned via an	2026-06-17	5.8	CVE-2026-48821

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	AJAX response and inserted into the DOM using innerHTML without proper sanitization. The issue originates from the interaction between the backend thumbnail update endpoint and the frontend JavaScript responsible for rendering update progress. On the backend, the ThumbnailsController::ajaxUpdate method returns bookmark data formatted using the 'raw' formatter. This includes the unescaped bookmark title in the JSON response. On the client side, the script thumbnails-update.js processes this AJAX response and dynamically updates the progress interface. Administrators using the thumbnail synchronization feature are affected and exploitation could lead to session hijacking, privilege escalation, backdoor injection and full compromise. This issue has been fixed in version 0.16.2.			
shaarli--Shaarli	Shaarli is a personal bookmarking service. Versions 0.16.1 and prior contain a stored Cross-Site Scripting (XSS) vulnerability in the Markdown-to-HTML conversion process used in the Bookmark Description field. An authenticated user can inject a malicious javascript: URI inside a Markdown link. The vulnerability originates in the filterProtocols method within BookmarkMarkdownFormatter.php. This method attempts to sanitize Markdown links by filtering dangerous protocols (such as javascript:) before rendering. It uses the following regular expression: <code>(#)\((.*?)\)#is</code>. This regex is designed to detect inline Markdown links, but it fails to detect Markdown reference-style links because reference-style links are resolved by the Markdown parser after preprocessing. The filterProtocols method never inspects the actual URL used in these references and as a result, an attacker can supply a javascript: URI inside a reference definition. This issue has been fixed in version 0.16.2.	2026-06-17	5.8	CVE-2026-48822
shaarli--Shaarli	Shaarli is a personal bookmarking service. Versions 0.16.1 and prior contain a stored Cross-Site Scripting (XSS) vulnerability in the tag filtering functionality of Shaarli. An authenticated user can inject arbitrary JavaScript into the tags field when creating a bookmark (Shaare). The malicious payload is stored and later executed when users interact with the "Filter by tag" search feature on the homepage. User-supplied input in the tags field is not properly sanitized or output-escaped before being rendered in the tag filtering interface. When a bookmark is created with a malicious payload inside the tag field, the payload is stored in the database. Later, when a user searches using the "Filter by tag" functionality on the homepage, the application renders matching tags dynamically. If the tag value contains HTML with JavaScript event handlers, it is injected into the DOM. This impacts anyone interacting with the "Filter by tag" search functionality, administrators and privileged users. This issue has been fixed in version 0.16.2.	2026-06-17	4.8	CVE-2026-48823
Shareaholic--Shareaholic	Missing Authorization vulnerability in Shareaholic allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Shareaholic: from n/a through 9.7.11.	2026-06-17	4.3	CVE-2024-24709
slimphp--Slim	Slim is a PHP micro framework that enables users to write simple web applications and APIs. In versions 4.4.0 through 4.15, if an application uses <code>HttpException::setTitle()</code> and/or <code>setDescription()</code> to include untrusted/request-derived data in the error title or description (e.g. "No products found matching '{\$query}'."), an attacker could inject arbitrary HTML/JavaScript that executes in the victim's browser when they encounter an HTML error page generated by Slim. The vulnerability is	2026-06-15	6.1	CVE-2026-48157

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	present even with <code>displayErrorDetails = false</code> as the unescaped title and description are rendered on this error path. Built-in exceptions (<code>HttpNotFoundException</code> , <code>HttpBadRequestException</code> , etc.) ship plain-text defaults, so a vanilla Slim app with no user code is not exploitable. Only applications that feed untrusted data into <code>setTitle()</code> and/or <code>setDescription()</code> are affected. The issue has been fixed in 4.15.2. If developers are unable to immediately update their applications, they can work around this issue by avoiding passing untrusted/request-derived data into <code>HttpException::setTitle()</code> and <code>setDescription()</code> and using static, plain-text error copy instead. They should also register a custom error renderer (an <code>ErrorRendererInterface</code> implementation, or a subclass of <code>HtmlErrorRenderer</code> that escapes the title and description) for the HTML media type.			
Splunk--Splunk AI Toolkit	In Splunk AI Toolkit versions below 5.7.4, a low-privileged user that does not hold the "admin" or "power" Splunk roles could cause the Splunk AI Toolkit to make outbound requests over HTTP to a server that an attacker controls, which could allow for data exfiltration. The vulnerability exists because of an insecure default domain allowlist in the Splunk AI Toolkit, which does not restrict outbound AI agent requests to approved external domains.	2026-06-17	4.3	CVE-2026-20265
statamic--cms	Statamic is a Laravel and Git powered content management system (CMS). Prior to 5.73.23 and 6.20.0, an authenticated Control Panel user could view metadata and content for resources they don't have permission to view, including entries, assets, users, roles, groups, and other configured resources. Depending on the resource, this could expose titles, custom field values, entry content, asset metadata, and the existence of users, roles, and groups. No data could be modified. This has been fixed in 5.73.23 and 6.20.0.	2026-06-19	4.3	CVE-2026-49288
SteeltoeOSS--Steeltoe.Configuration.Abstractions	Steeltoe is an open source project that provides a collection of libraries that helps users build cloud-native applications. In Steeltoe.Configuration.Abstractions 4.0.0 through 4.1.0, when MySQL or PostgreSQL service bindings from `VCAP_SERVICES` include TLS client credentials, the Connectors library writes those credentials to temporary files in <code>Path.GetTempPath()</code> using <code>File.CreateText</code> . On Linux, <code>File.CreateText</code> creates files with mode <code>0644</code> (world-readable) under the process umask, and the files are never deleted. The same key material is protected at mode <code>0400</code> in <code>/proc/<pid>/environ</code> . Steeltoe.Configuration.Abstractions version 4.2.0 patches the issue. If an immediate upgrade is not possible, prevent other processes from running in the container under a different UID with access to <code>/tmp</code> .	2026-06-17	4.7	CVE-2026-50267
SteeltoeOSS--Steeltoe.Management.Endpoint	Steeltoe is an open source project that provides a collection of libraries that helps users build cloud-native applications. In Steeltoe.Management.Endpoint prior to version 4.2.0 and Steeltoe.Management.EndpointCore prior to version 3.4.0, all Steeltoe actuator endpoints default to <code>EndpointPermissions.Restricted</code> , which is mapped to Cloud Foundry's <code>read_basic_data</code> permission (granted to Space Auditors and similar low-trust roles). Sensitive actuators including heap dump, environment, and thread dump do not raise this to <code>EndpointPermissions.Full</code> , so CF's <code>read_sensitive_data</code> permission flag is not enforced for those endpoints. Spring Boot's equivalent Cloud Foundry integration gates these endpoints with <code>read_sensitive_data</code> by default.	2026-06-17	6.5	CVE-2026-50201

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Steeltoe.Management.Endpoint 4.2.0 and Steeltoe.Management.EndpointCore 3.4.0 patch the issue. If an immediate upgrade is not possible, explicitly set `RequiredPermissions = EndpointPermissions.Full` in the options for `HeapDumpEndpointOptions`, `EnvironmentEndpointOptions`, and `ThreadDumpEndpointOptions`; and/or if heap dump, thread dump, or environment are not needed in production, register only the required actuators individually instead of using `AddAllActuators()`.			
SteeltoeOSS-- Steeltoe.Security.Authentication.CloudFoundryBase	Steeltoe is an open source project that provides a collection of libraries that helps users build cloud-native applications. In Steeltoe.Security.Authentication.CloudFoundryBase prior to version 3.4.0, Steeltoe.Security.Authentication.JwtBearer prior to version 4.2.0, and Steeltoe.Security.Authentication.OpenIdConnect prior to version 4.2.0, the JWT signing key cache in `TokenKeyResolver` uses `kid` as the sole cache key without namespacing by authority. In applications with multiple `JwtBearer` schemes pointing to different identity providers, a key fetched for one scheme can satisfy token validation for another. Additionally, cached keys have no expiration, so rotated or revoked keys remain trusted until the application process restarts. Steeltoe.Security.Authentication.CloudFoundryBase version 3.4.0, Steeltoe.Security.Authentication.JwtBearer version 4.2.0, and Steeltoe.Security.Authentication.OpenIdConnect version 4.2.0 patch the issue. If an immediate upgrade is not possible: In multi-scheme deployments, configure only one `JwtBearer` scheme per application when different identity providers are required; and/or restart the application process after an identity provider signing key rotation to clear stale cached keys.	2026-06-17	5.9	CVE-2026-50202
stellarwp-- Kadence Blocks Page Builder Toolkit for Gutenberg Editor	The Kadence Blocks - Page Builder Toolkit for Gutenberg Editor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.7.5 via the editor_assets_variables. This makes it possible for authenticated attackers, with contributor-level access and above, to extract the site's connected Kadence account license key, license owner email, api_key, api_email, and license domain from the browser console by inspecting window.kadence_blocks_params.proData. Exploitation requires only that an administrator has previously connected a valid Kadence license; the full credential bundle is then readable by any Contributor-level user from the block editor client context without any server-side request manipulation.	2026-06-18	4.3	CVE-2026-11357
strablengineerin g--STRABL A checkout solution	The STRABL - A checkout solution plugin for WordPress is vulnerable to Missing Authentication in all versions up to and including 4.5. The plugin registers a REST API webhook endpoint at /wp-json/strabl/webhook/order with a permission_callback of __return_true, which allows all incoming requests without any authentication or authorization checks. No shared secret, signature validation, HMAC verification, or token-based authentication is implemented. This makes it possible for unauthenticated attackers to create fraudulent WooCommerce orders and mark them as completed by supplying paymentStatus=paid, manipulate existing order statuses by providing an externalOrderId, create new WordPress user accounts with the customer role, issue refunds on existing orders, cancel existing orders, and apply chargeback fees - all without making a legitimate payment or having any valid credentials.	2026-06-19	5.3	CVE-2026-3640

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
strukturag--libde265	libde265 is an open source implementation of the h.265 video codec. Prior to version 1.0.20, a crafted sequence of H.265 NAL units causes `decoder_context::read_slice_NAL()` (`libde265/deccctx.cc:481`) to attach slice headers to a finished picture object that has no active image unit, resulting in attacker-controlled unbounded heap growth. The retained headers are never freed until the picture is released, which may not happen during continuous streaming. Version 1.0.20 patches the issue.	2026-06-19	4.3	CVE-2026-49337
strukturag--libheif	libheif is a HEIF and AVIF file format decoder and encoder. Prior to version 1.22.1, the uncompressed HEIF decoder validates explicit icf compressed-unit offsets using unit_offset + unit_size. Because the addition can wrap, a crafted HEIF file can pass the range check and then construct a vector from iterators outside the compressed item buffer, producing an out-of-bounds heap read and crash. Version 1.22.1 patches the issue.	2026-06-19	6.5	CVE-2026-49271
StylemixThemes--MasterStudy LMS Pro	Missing Authorization vulnerability in StylemixThemes MasterStudy LMS Pro allows Accessing Functionality Not Properly Constrained by ACLs. This issue affects MasterStudy LMS Pro: from n/a before 4.7.16.	2026-06-15	6.5	CVE-2025-64215
StylemixThemes--Motors	Subscriber Broken Access Control in Motors < 1.4.107 versions.	2026-06-15	6.5	CVE-2026-39515
SUSE--libzyp	A path traversal in handling the "path" component of .repo files processed by libzyp before 17.38.13 in the 17.x series, or before 16.22.19 could be used by attackers to fill directories on the system outside of the zyp cache with content.	2026-06-18	6.5	CVE-2026-44942
svaara--duktape	A weakness has been identified in svaara duktape up to 2.99.99. This issue affects some unknown processing of the file duk_api_bytecode.c. Executing a manipulation of the argument count_instr can lead to memory corruption. The attack requires local access. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	5.3	CVE-2026-12216
teamwsa--Woosa Marktplaats for WooCommerce	The Woosa - Marktplaats for WooCommerce plugin for WordPress is vulnerable to Arbitrary File Read via Path Traversal in versions up to and including 2.0.4. This is due to insufficient path sanitization in the render_logs_ui() function, which accepts a base64-encoded file name from the 'log_file' GET parameter and concatenates it directly with the plugin's log directory path without validating that the resolved path remains within the intended directory. This makes it possible for authenticated attackers, with Administrator-level access, to read the contents of arbitrary files on the server, including wp-config.	2026-06-19	4.9	CVE-2026-7547
techlabpro1--Classified Listing AI-Powered Classified ads & Business Directory	The Classified Listing - Classified ads & Business Directory plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 5.4.2. This is due to a missing capability/ownership check on the gallery_image_update_as_feature AJAX handler (action: rtcl_fb_gallery_image_update_as_feature), which accepts a user-supplied listing ID and attachment ID and sets the featured image of a listing while only validating a nonce that is exposed to any logged-in user on the frontend listing-submission form. This makes it possible for authenticated attackers, with Subscriber-level access and above, to change the featured image of arbitrary listings they do not own.	2026-06-19	4.3	CVE-2026-10779

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Themefic--Ultra Addons for WPForms	Subscriber Broken Access Control in Ultra Addons for WPForms <= 1.0.11 versions.	2026-06-15	6.4	CVE-2026-39594
ThemeGrill--Masteriyo - LMS	Unauthenticated Broken Authentication in Masteriyo - LMS <= 2.1.8 versions.	2026-06-15	6.5	CVE-2026-42743
themeisle--Orbit Fox: Duplicate Page, Menu Icons, SVG Support, Cookie Notice, Custom Fonts & More	The Orbit Fox: Duplicate Page, Menu Icons, SVG Support, Cookie Notice, Custom Fonts & More plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.0.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2026-06-18	4.4	CVE-2026-11358
Themeisle--WP Full Stripe Free	Subscriber Broken Authentication in WP Full Stripe Free <= 8.4.1 versions.	2026-06-15	6.5	CVE-2026-42378
Themeum--Tutor LMS	Unauthenticated Broken Access Control in Tutor LMS <= 3.9.7 versions.	2026-06-15	6.5	CVE-2026-40743
themeum--Tutor LMS eLearning and online course solution	The Tutor LMS - eLearning and online course solution plugin for WordPress is vulnerable to generic SQL Injection via the 'data' parameter in all versions up to, and including, 3.9.11 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-06-18	4.9	CVE-2026-10736
thorsten--phpMyFAQ	phpMyFAQ is an open source FAQ web application. Versions prior to 4.1.4 have Missing Authorization in the API CategoryController. CVE-2026-24421 addressed this in the BackupController by adding: \$this->userHasPermission(PermissionType::BACKUP). The same fix was not applied to 4 other write endpoints in the public API. All 4 only call \$this->hasValidToken() - which checks a shared API key header, rather than the individual user's role permissions. The following APIs are affected: POST /api/v4.0/category (CategoryController::create), POST /api/v4.0/faq (FaqController::create), PUT /api/v4.0/faq (FaqController::update), and POST /api/v4.0/question (QuestionController::create). This issue has been fixed in version 4.1.4.	2026-06-18	6.5	CVE-2026-49205
TMS--Amelia	Subscriber Broken Access Control in Amelia <= 2.2 versions.	2026-06-15	6.5	CVE-2026-40795
ts-deepmerge--ts-deepmerge	Versions of the package ts-deepmerge before 8.0.0 are vulnerable to Uncaught Exception due to the improper handling of built-in Object.prototype methods (such as toString, valueOf). When user-controlled input contains these keys with non-function values, the resulting merged object becomes broken - any string context operation throws a TypeError, crashing the application.	2026-06-19	5.3	CVE-2026-12644
typemill--typemill	Typemill before 2.24.0 contains a path traversal vulnerability that allows authenticated attackers with Author-level privileges to read arbitrary files outside the content directory by supplying traversal sequences in the path	2026-06-17	6.5	CVE-2026-49133

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	query parameter passed to Storage::getFile() with an empty folder argument. Attackers can bypass traversal-prevention controls in Storage::getFolderPath() to access sensitive files.			
undici--undici	Impact: Undici's cache interceptor incorrectly classifies some responses as cacheable when the upstream Cache-Control header uses whitespace-padded qualified private or no-cache field names such as private=" authorization" or no-cache="\tauthorization". The parser preserves the surrounding whitespace, so later comparisons against the literal authorization field name fail and the response is stored. In shared-cache mode, this allows a response containing one user's authenticated data to be served from cache to a subsequent caller, including an unauthenticated caller, when both requests resolve to the same cache key. Affected applications are those that explicitly enable the cache interceptor (interceptors.cache()) in shared mode, forward Authorization headers upstream, and receive cacheable responses with non-canonical qualified private or no-cache directives. Patches: Upgrade to undici v7.28.0 or v8.5.0. Workarounds: If upgrade is not immediately possible, disable shared-cache mode for traffic that includes Authorization headers, avoid caching responses to authenticated requests, or add Vary: Authorization upstream.	2026-06-17	5.9	CVE-2026-9678
undici--undici	Impact: undici's cookie parser in parseSetCookie percent-decodes cookie values via qsUnescape, turning encoded sequences like %0D%0A, %00, %3B, and %3D into their literal byte equivalents. RFC 6265 §5.4 does not specify any decoding and browsers do not decode either. Applications that parse a Set-Cookie header and then forward the parsed value into a response header (proxies, middleware, SSR frameworks) become vulnerable to HTTP response header injection: an attacker-controlled upstream can inject arbitrary Set-Cookie, Location, or Cache-Control headers into the application's downstream response, enabling session fixation, open redirect, or cache poisoning. Affected applications are those that use undici's cookie parsing (parseSetCookie, parseCookie, getSetCookies) and forward the parsed cookie value into a response header. This was introduced in undici 7.0.0 via PR #3789. Patches: Upgrade to undici v6.26.0, v7.28.0 or v8.5.0. Workarounds: If upgrade is not immediately possible, do not forward values returned by parseSetCookie/parseCookie/getSetCookies directly into response headers; sanitize the value first to strip or reject CR, LF, NUL, ,, and = bytes.	2026-06-17	5.9	CVE-2026-9679
universal-tool-calling-protocol--python-utcp	A vulnerability was detected in universal-tool-calling-protocol python-utcp 1.1.0. This affects an unknown function of the component utcp-gql/utcp-websocket. Performing a manipulation results in server-side request forgery. The attack can be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	6.3	CVE-2026-12210
valhalla--valhalla	Valhalla is an open source routing engine and accompanying libraries for use with OpenStreetMap data. Versions 3.6.3 and prior are vulnerable to reflected cross-site scripting (XSS) due to improper neutralization of input in the JSONP callback parameter. When a request specifies a JSONP callback, the value is reflected directly into the HTTP response body with Content-Type: application/javascript, without any validation, output encoding, or allowlist filtering. An attacker can craft a URL containing arbitrary JavaScript in the callback parameter; if a victim is induced to load	2026-06-15	6.1	CVE-2026-49294

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	that URL via a <script src="..."> tag, the injected script executes in the context of the serving origin, potentially leading to session token theft, credential disclosure, or actions performed on behalf of the victim. This issue was not fixed at time of publication.			
VeronaLabs--Slimstat Analytics	Unauthenticated Deserialization of untrusted data in Slimstat Analytics < 5.4.0 versions.	2026-06-17	6.5	CVE-2026-27410
VeronaLabs--WP SMS	Subscriber Sensitive Data Exposure in WP SMS <= 7.2.1 versions.	2026-06-15	6.5	CVE-2026-40790
virtio-snd device--virtio-snd device	An integer overflow vulnerability was found in the virtio-snd device via PCM_INFO requests from the guest. A malicious guest can provide out-of-bounds stream counts, potentially leading to unbounded memory allocation on the host and a denial of service condition.	2026-06-19	5.5	CVE-2026-3196
vllm--vllm	vLLM versions >= 0.6.3 and < 0.9.0 contain multiple regular expression denial of service (ReDoS) vulnerabilities. Several regex patterns - in vllm/lora/utils.py, the phi4mini tool parser, and the OpenAI-compatible serving chat endpoint - are susceptible to catastrophic backtracking. An attacker submitting crafted input with nested or repeated structures can trigger severe CPU consumption and performance degradation, resulting in denial of service.	2026-06-20	4.3	CVE-2025-71379
vynnus--PopAd	Administrator Server Side Request Forgery (SSRF) in PopAd <= 1.0.4 versions.	2026-06-15	4.4	CVE-2025-60175
Wasiliy Strecker--Contest Gallery	Subscriber Cross Site Scripting (XSS) in Contest Gallery <= 28.1.6 versions.	2026-06-15	6.5	CVE-2026-42656
Wasiliy Strecker--Contest Gallery	Unauthenticated Other Vulnerability Type in Contest Gallery <= 28.1.7 versions.	2026-06-15	6.5	CVE-2026-42657
Wasiliy Strecker--Contest Gallery	Subscriber Sensitive Data Exposure in Contest Gallery <= 28.1.7 versions.	2026-06-15	6.5	CVE-2026-42660
watchful--XCloner	Subscriber Sensitive Data Exposure in XCloner <= 4.8.6 versions.	2026-06-15	6.5	CVE-2026-48965
Webful Creations--RepairBuddy	Subscriber Broken Access Control in RepairBuddy <= 4.1132 versions.	2026-06-15	6.5	CVE-2026-39584
Webmin--Webmin	Webmin allows unauthenticated attackers to read the contents of any file ending in .conf within module directories, due to a bypassable regex pattern.	2026-06-18	5.3	CVE-2026-56021
Webmin--Webmin	Webmin accepts basic authentication without session cookies when an attacker provides the 'User-Agent: webmin' header, allowing bypass of additional MFA requirements. Fixed in 2.641.	2026-06-18	5.3	CVE-2026-56022
webpack-dev-server--webpack-dev-server	Impact: When a user-configured proxy on webpack-dev-server has a broad context (e.g. /) and ws: true, it also intercepts the dev server's own HMR WebSocket and forwards it to the proxy target. This leaks the browser's cookies and Origin header to the backend, bypasses the dev server's Host/Origin validation, and corrupts the HMR socket (both HMR and the proxy end up writing to the same socket). Patches: Fixed in webpack-dev-	2026-06-15	5.3	CVE-2026-9595

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	server@5.2.5. Workarounds: Scope user-defined proxy context to specific paths instead of /, or omit ws: true from the proxy entry when WebSocket forwarding is not required.			
WishList Member-- WishList Member X	Subscriber Broken Access Control in WishList Member X <= 3.29.0 versions.	2026-06-17	4.3	CVE-2026-24575
woocommerce-- WooCommerce Stripe Payment Gateway	The WooCommerce Stripe Payment Gateway plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the `ajax_pay_for_order()` function in all versions up to, and including, 10.7.0 This is due to a missing order ownership or order_key verification when processing payment for an order via the `wc_stripe_pay_for_order` WC-AJAX endpoint. The function only validates a nonce (which is publicly available on any WooCommerce page where Express Checkout is enabled), but does not verify that the requesting user owns the target order and is allowed to modify it. This makes it possible for unauthenticated attackers to force any pending order into a failed status by providing a fake payment method, causing a payment exception that updates the order status to "failed" via sequential order ID enumeration.	2026-06-16	6.5	CVE-2026-2381
WP Chill-- Download Monitor	Author Arbitrary File Download in Download Monitor <= 5.1.9 versions.	2026-06-15	4.4	CVE-2026-39489
WP Chill-- Modula Image Gallery	Subscriber Cross Site Scripting (XSS) in Modula Image Gallery <= 2.14.23 versions.	2026-06-15	6.5	CVE-2026-42688
WP Engine--WP Migrate Lite	Unauthenticated Cross Site Request Forgery (CSRF) in WP Migrate Lite <= 2.7.8 versions.	2026-06-15	4.7	CVE-2026-49043
wp.insider-- Simple Membership	Unauthenticated Cross Site Scripting (XSS) in Simple Membership <= 4.7.2 versions.	2026-06-15	6.5	CVE-2026-42663
wpcalc--Counter Box Add Countdowns, Timers & Dynamic Counters to WordPress	The Counter Box - Add Countdowns, Timers & Dynamic Counters to WordPress plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.0.13 via deserialization of untrusted input . This makes it possible for authenticated attackers, with administrator-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software, which means this vulnerability has no impact unless another plugin or theme containing a POP chain is installed on the site. If a POP chain is present via an additional plugin or theme installed on the target system, it may allow the attacker to perform actions like delete arbitrary files, retrieve sensitive data, or execute code depending on the POP chain present. Deserialization is triggered automatically upon the post-import redirect that renders the list table, and again when any item is opened for editing, requiring no additional navigation beyond the import action itself.	2026-06-17	6.6	CVE-2026-12115

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
WPDeveloper-- Essential Addons for Elementor	Unauthenticated Broken Access Control in Essential Addons for Elementor < 6.6.0 versions.	2026-06-15	5.3	CVE-2026-25440
wpdevteam-- BetterDocs AI Documentation, Knowledge Base, Docs, Wikis, FAQ with Chatbot	The BetterDocs - Knowledge Base Docs & FAQ Solution for Elementor & Block Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the blockId attribute of the betterdocs/category-slate-layout Gutenberg block in versions up to, and including, 4.5.3. This is due to insufficient input sanitization and output escaping in the CategorySlateLayout::render() method, which echoes the blockId block attribute directly into an HTML class attribute without esc_attr(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-19	6.4	CVE-2026-12157
wpgmaps--WP Go Maps Google Map, OpenStreetMap, Leaflet Map	The WP Go Maps - Most Popular Map Plugin plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 10.1.01. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to create arbitrary records in plugin database tables (maps, markers, circles, polygons, polylines, rectangles, and point labels) by supplying a WPGMZA-namespaced CRUD-backed class name via the phpClass parameter. The namespace validation check (requiring the 'WPGMZA' prefix) does not prevent exploitation because classes such as WPGMZA\Map and WPGMZA\Marker satisfy it while still triggering an INSERT into the corresponding plugin table before the route rejects the request.	2026-06-19	5.3	CVE-2026-12238
wpinsider-1-- Simple Membership	The Simple Membership plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.7.5. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to deactivate arbitrary member accounts by forging a charge.refunded webhook event containing a victim's subscription ID, setting the target member's account_state to 'inactive' and triggering cancellation hooks, transaction-record status changes, and cancellation notification emails. This vulnerability is exploitable only on installations where no Stripe webhook signing secret has been configured, which is the default out-of-the-box state; sites that have configured the stripe-webhook-signing-secret option are routed to the properly verified HMAC path and are not affected.	2026-06-18	5.3	CVE-2026-12093
Wpmet-- GetGenie	Unauthenticated Sensitive Data Exposure in GetGenie <= 4.4.1 versions.	2026-06-16	6.5	CVE-2026-54197
WPMet-- MetForm Pro	Subscriber Broken Access Control in MetForm Pro <= 3.9.1 versions.	2026-06-17	4.3	CVE-2026-24610
wproyal--Royal Addons for Elementor Addons and Templates Kit for Elementor	The Royal Addons for Elementor - Addons and Templates Kit for Elementor plugin for WordPress is vulnerable to Arbitrary File Read in versions 1.7.1058 through 1.7.1059. This is due to the wpr_get_csv_handle() helper (introduced in version 1.7.1058 as part of the patch for CVE-2026-6229) falling back to is_readable() and fopen(\$source, 'r') on the attacker-controlled settings.table_upload_csv.url value when it does not parse as an HTTP URL, with no allow-list, traversal block, or extension check. This makes it possible for authenticated attackers, with Contributor-level	2026-06-19	6.5	CVE-2026-8118

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	access and above, to save a crafted wpr-data-table widget through Elementor's save_builder endpoint and have the rendered preview return the line-by-line contents of any file readable by the PHP process, including wp-config.php.			
WWBN--AVideo	AVideo TopMenu plugin through version 26.0 contains a stored cross-site scripting vulnerability in menu item rendering due to missing output encoding of icon classes, URLs, and text labels. Attackers can inject malicious JavaScript through unescaped menu item fields that execute for all site visitors, potentially stealing session cookies or performing unauthorized actions.	2026-06-20	6.1	CVE-2026-56347
XianYuLauncher--XianYuLauncher	XianYuLauncher is a Minecraft Java Edition launcher. In versions prior to 1.5.5, sensitive authentication artifacts could be exposed during a user-initiated login under certain local attack conditions. Affected versions relied on a fixed localhost redirect URI without PKCE or state validation. Exploitation is most likely to occur when an attacker is able to observe, intercept, or otherwise interfere with the local authentication flow on the same device. This issue has been fixed in version 1.5.5.	2026-06-17	5.5	CVE-2026-48991
Yealink--SIP-T46U	A flaw has been found in Yealink SIP-T46U 108.86.0.118. The impacted element is the function mod_diagnose.CommandShellByType of the file /api/diagnosis/start of the component Web FastCGI Service. This manipulation of the argument Time causes command injection. The attack can be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	6.3	CVE-2026-12219
Yealink--SIP-T46U	A vulnerability was identified in Yealink SIP-T46U 108.86.0.118. Affected by this vulnerability is the function mod_webd.TFTPUplodlperf of the file /api/inner/tftpuploadiperf of the component Web FastCGI Service. The manipulation of the argument ip/port leads to command injection. The attack needs to be initiated within the local network. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	5.5	CVE-2026-12223
Yoast BV--Yoast SEO Premium	Missing Authorization vulnerability in Yoast BV Yoast SEO Premium allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Yoast SEO Premium: from n/a through 26.6.	2026-06-17	5.5	CVE-2026-40722
zealopensource--Abandoned Contact Form 7	The Abandoned Contact Form 7 plugin for WordPress is vulnerable to unauthorized arbitrary post deletion in versions up to, and including, 2.2. This is due to a missing capability check and missing nonce validation in the action__remove_abandoned() function, which is registered to both the wp_ajax_remove_abandoned and wp_ajax_nopriv_remove_abandoned hooks. The handler takes a user-supplied recover_id parameter from \$_POST and passes it directly to wp_delete_post() with the force-delete flag set to true, without verifying that the ID belongs to the plugin's own cf7af_data post type. This makes it possible for unauthenticated attackers to permanently delete arbitrary posts, pages, or other content on the affected site by sending a single admin-ajax.	2026-06-16	5.3	CVE-2026-9187
zephyrproject--zephyr	On Xtensa targets with CONFIG_USERSPACE and CONFIG_XTENSA_MMU, the page-table code (arch/xtensa/core/ptables.c) maintains a global list, xtensa_domain_list, of active memory domains using a list node embedded inside the caller-owned struct k_mem_domain. When a domain	2026-06-16	6.3	CVE-2026-10635

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	is destroyed via <code>k_mem_domain_deinit()</code> - <code>arch_mem_domain_deinit()</code>, the page tables are torn down and <code>domain-arch.ptables</code> is set to <code>NULL</code>, but the domain's node was not removed from <code>xtensa_domain_list</code>. The freed/deinitialized domain therefore remained linked into the global list as a dangling pointer into caller-owned storage that may then be freed or reused. Any subsequent <code>arch_mem_map()/arch_mem_unmap()</code> operation (widely invoked by kernel memory-mapping and demand-paging code) traverses the stale node and dereferences <code>domain-ptables</code>: at minimum a <code>NULL</code> pointer dereference causing a fatal MMU exception (denial of service), and if the <code>k_mem_domain</code> storage has been freed or reused, a use-after-free in which a stale/controlled <code>ptables</code> value is dereferenced and written through during the page-table walk (<code>l2_page_table_map</code> writes <code>l1_table[...]</code> and <code>l2_table[...]</code>, and <code>xtensa_mmu_compute_domain_regs</code> writes into the domain struct and the L1 table), yielding page-table memory corruption that can undermine userspace isolation. The vulnerable path is reachable only from privileged kernel/supervisor code (<code>k_mem_domain_deinit</code> is not a syscall), not directly from unprivileged user threads or remotely. Affected: Zephyr v4.4.0 (the Xtensa memory-domain de-initialization feature was introduced in commit 3032b58f52d and first shipped in v4.4.0); fixed on main by adding <code>sys_slist_find_and_remove()</code> in <code>arch_mem_domain_deinit()</code>. The Xtensa MPU path is unaffected.			
zephyrproject--zephyr	<code>subsys/net/ip/ipv6_mld.c:mld_send()</code> read the packet interface via <code>net_pkt_iface(pkt)</code> after <code>net_send_data(pkt)</code> returned successfully. Per the network stack's ownership contract (include/zephyr/net/net_core.h, and the explicit warning in <code>subsys/net/ip/net_core.c:453-460</code> 'do not use <code>pkt</code> after that call'), a successful send transfers ownership of the <code>net_pkt</code> and the L2 driver frees it (e.g. <code>ethernet_send()</code> unrefs the packet on success, <code>subsys/net/l2/ethernet/ethernet.c:790</code>), returning it to its <code>k_mem_slab</code>. The subsequent <code>net_pkt_iface(pkt)</code> is therefore a read of a freed object; the recovered interface pointer is then dereferenced and incremented by the per-interface statistics path (<code>net_stats.h</code> <code>UPDATE_STAT/SET_STAT</code>) when <code>CONFIG_NET_STATISTICS_PER_INTERFACE</code> is enabled. If the freed slot is concurrently reallocated, <code>pkt-iface</code> may read back as <code>NULL</code> (<code>NULL</code>-pointer dereference / crash) or as a stale/garbage pointer (stray increment write / memory corruption). The path is reachable remotely on the local link without authentication: <code>handle_mld_query()</code> (registered for <code>NET_ICMPV6_MLD_QUERY</code>) responds to a valid MLDv2 General Query (unspecified multicast address, hop limit 1) by calling <code>send_mld_report()</code> - <code>mld_send()</code>. The result is a remotely triggerable denial of service of the networking stack, with a narrow possibility of memory corruption. The fix caches the interface in a local before sending and no longer touches the packet after <code>net_send_data()</code>. The IPv4/IGMP sibling (<code>igmp_send</code>) already used the corrected pattern.	2026-06-16	5.9	CVE-2026-10637
zephyrproject--zephyr	<code>subsys/net/ip/icmpv6.c</code> reads the network interface from a <code>net_pkt</code> after that packet has been handed to <code>net_try_send_data()</code>. In <code>icmpv6_handle_echo_request()</code> and <code>net_icmpv6_send_error()</code>, the post-send statistics update calls <code>net_pkt_iface(reply)/net_pkt_iface(pkt)</code> on the just-sent packet. The send path (<code>net_try_send_data</code> - <code>net_if_tx</code>) unreferences and may free the packet back to its memory slab before returning - synchronously in the RX thread when no TX queue is configured (<code>CONFIG_NET_TC_TX_COUNT == 0</code>), and asynchronously the driver/L2 may	2026-06-16	5.9	CVE-2026-10638

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	already have freed it otherwise. <code>net_pkt_iface()</code> therefore dereferences a freed (and possibly reused) <code>net_pkt</code>; with <code>CONFIG_NET_STATISTICS_PER_INTERFACE</code> the stale <code>iface</code> pointer is further dereferenced and written through (<code>iface-stats.icmp.sent++</code>), turning the use-after-free read into a write through an attacker-influenceable pointer. The core stack already documents this hazard in <code>net_core.c</code> ("do not use <code>pkt</code> after that call") and caches <code>iface</code> before sending; the ICMPv6 callers did not. An unauthenticated remote attacker triggers the flaw simply by sending an ICMPv6 Echo Request (ping) or an IPv6 packet that elicits an ICMPv6 error (unknown next header, fragment reassembly timeout, destination unreachable), leading to denial of service via crash and potential memory corruption. Affected: Zephyr networking with <code>CONFIG_NET_NATIVE_IPV6</code>, roughly v4.2.0 through v4.4.0. The fix caches the interface pointer before sending and uses it for all statistics updates; the sibling commit 86e21665d46 fixes the identical bug in ICMPv4.			
zephyrproject-zephyr	Zephyr's native TCP stack iterates the global connection list in <code>net_tcp_foreach()</code> (<code>subsys/net/ip/tcp.c</code>) using the <code>SYS_SLIST_FOR_EACH_CONTAINER_SAFE</code> macro, which caches a pointer to the next list node. Prior to this fix the function released <code>tcp_lock</code> while invoking the per-connection callback and re-acquired it afterwards. During that window a concurrent <code>tcp_conn_release()</code>, running on the dedicated TCP work-queue thread when a connection's reference count drops to zero (e.g. a remote peer closing or resetting the connection), can remove and <code>k_mem_slab_free()</code> the cached next connection. When the iterator advances it dereferences the freed (and possibly reallocated) slab memory - a use-after-free that can crash the system (denial of service) and, if the slot has been reused, cause the callback to operate on an attacker-influenced object (potential information disclosure or further fault). <code>net_tcp_foreach()</code> is reached in production via the 'net conn' network shell command and via <code>net_tcp_close_all_for_iface()</code> on interface-down; the freeing side is driven by ordinary TCP traffic. The fix moves the connection/context teardown in <code>tcp_conn_release()</code> inside the <code>tcp_lock</code> critical section and keeps <code>tcp_lock</code> held across the callback in <code>net_tcp_foreach()</code>. The defect was introduced with the modern (TCP2) stack in 2020 and affects releases up to and including v4.4.0.	2026-06-15	4.8	CVE-2026-10634
zephyrproject-zephyr	In Zephyr's native IPv4 stack, <code>icmpv4_handle_echo_request()</code> in <code>subsys/net/ip/icmpv4.c</code> builds an echo-reply packet (reply), hands it to <code>net_try_send_data()</code>, and then, on success, calls <code>net_stats_update_icmp_sent(net_pkt_iface(reply))</code>. <code>net_try_send_data()</code> transfers ownership of reply to the TX path (<code>net_if_try_queue_tx</code> - <code>net_if_tx</code> - L2/driver send, or the asynchronous <code>net_if_tx_thread</code>), which can unref it to refcount 0 and return the struct <code>net_pkt</code> to its slab (<code>net_pkt_unref</code> - <code>k_mem_slab_free</code>) before the stats line runs. <code>net_core.c</code> documents this exact contract ('the <code>pkt</code> might contain garbage already ... do not use <code>pkt</code> after that call'). The post-send <code>net_pkt_iface(reply)</code> therefore reads reply-<code>iface</code> out of a freed (and possibly already reallocated) <code>net_pkt</code>, a use-after-free read; with <code>CONFIG_NET_STATISTICS_PER_INTERFACE</code> the stats macro additionally increments a counter through that value, i.e. a dereference/write through a stale or recycled-slot pointer. The path is reached unauthenticated by any remote host that pings the device (<code>net_icmpv4_input</code> - <code>net_icmp_call_ipv4_handlers</code> - <code>icmpv4_handle_echo_request</code>) and is gated	2026-06-16	4.8	CVE-2026-10639

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	on CONFIG_NET_STATISTICS_ICMP. Impact is a probabilistic read of recycled packet memory plus a possible wild-pointer write under a timing race, leading most likely to corrupted interface statistics or a remotely triggerable crash (DoS). The defect was introduced in 2019 (v1.14) and is present through v4.4.0. The companion change in net_icmpv4_send_error() is not a use-after-free because it reads net_pkt_iface(orig), the caller-owned received packet, which stays alive across the send. The fix caches the interface pointer from the live received packet before sending and uses it for the post-send stats updates.			
zephyrproject--zephyr	Zephyr's IPv6 Neighbor Discovery send paths (net_ipv6_send_na, net_ipv6_send_ns, net_ipv6_send_rs in subsys/net/ip/ipv6_nbr.c) updated the per-interface ICMP-sent statistics by calling net_pkt_iface(pkt) after net_send_data(pkt) had already returned successfully. On the success path the network stack owns and releases the packet's reference (the L2/driver send unrefs it, e.g. ethernet_send - net_pkt_unref), so for a freshly allocated packet with refcount 1 the net_pkt slab block can be freed before the statistics line runs (synchronously when no TX queue thread is configured, or via a concurrent TX thread otherwise). The subsequent net_pkt_iface(pkt) reads pkt_iface from the freed slab block, and with CONFIG_NET_STATISTICS_PER_INTERFACE enabled that loaded pointer is dereferenced to increment iface-stats.icmp.sent, a use-after-free (CWE-416). If the slab block was reallocated in the meantime the read/increment targets unrelated or attacker-influenced memory, yielding corrupted statistics, a fault/crash (denial of service), or potential limited memory corruption. The vulnerable Neighbor Advertisement path is reachable by any unauthenticated on-link node simply by sending ICMPv6 Neighbor Solicitations to a Zephyr node with native IPv6 enabled (handle_ns_input - net_ipv6_send_na). Affected from v3.3.0 through v4.4.0; the fix uses the already-available iface argument instead of touching the sent packet. Configurations without per-interface statistics dereference only a global counter and are not affected by the memory-safety aspect.	2026-06-16	4.2	CVE-2026-10640
zhilink ()--ADP Application Developer Platform	A vulnerability was found in zhilink æ™ªä'è"(æ·±æ³)ç\$'æšææ%œé™ªâ...-â, ADP Application Developer Platform â"ç""â¼æâ'è€...â¹â° 1.0.0. This affects an unknown part of the component testConnection Endpoint. The manipulation of the argument jdbcUrl results in deserialization. The attack may be performed from remote. The exploit has been made public and could be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	6.3	CVE-2026-12787
zhilink ()--ADP Application Developer Platform	A vulnerability was determined in zhilink æ™ªä'è"(æ·±æ³)ç\$'æšææ%œé™ªâ...-â, ADP Application Developer Platform â"ç""â¼æâ'è€...â¹â° 1.0.0. This vulnerability affects unknown code of the file /adpweb/a/base/barcodeDetail/import of the component XML Parser. This manipulation causes xml external entity reference. It is possible to initiate the attack remotely. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	6.3	CVE-2026-12788
1Panel-dev--MaxKB	MaxKB before 2.10.0 contains a server-side request forgery vulnerability in tool creation and update endpoints that allows authenticated users to make arbitrary server requests by supplying unvalidated downloadCallbackUrl and download_url parameters. Attackers with	2026-06-25	6.4	CVE-2026-56779

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	default workspace USER role can exploit this to access internal network services by providing malicious URLs to the ToolSerializer endpoints.			
24liveblog-- 24liveblog live blog tool	The 24liveblog - live blog tool plugin for WordPress is vulnerable to Exposure of Sensitive Information in versions up to, and including, 2.2. This is due to the lb24_block_enqueue_scripts() function being hooked to enqueue_block_editor_assets and, for any non-administrator user, falling back to loading the administrator-configured site-wide 24liveblog integration secrets (lb24_token, lb24_refresh_token, lb24_uid, lb24_uname) from the options table via get_option() and emitting them through wp_localize_script() as the lb24BlockData JavaScript object. This makes it possible for authenticated attackers, with contributor-level access and above, to extract third-party 24liveblog account credentials (including the API token and refresh token) by simply opening the block editor and inspecting the page source.	2026-06-24	4.3	CVE-2026-9183
24liveblog-- 24liveblog live blog tool	The 24liveblog - live blog tool plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the update_lb24_token() AJAX function in versions up to, and including, 2.2. The handler only verifies the 'lb24' nonce (which is generated and localized to any user with block editor access via lb24_block_enqueue_scripts()) and does not verify the user's capabilities or that the supplied user_id belongs to the current user. This makes it possible for authenticated attackers, with author-level access and above, to overwrite the lb24_token, lb24_uid, lb24_refresh_token, and lb24_uname user meta values of any user (including administrators) as well as the corresponding site-wide options, effectively hijacking the plugin's integration with the 24liveblog service.	2026-06-24	4.3	CVE-2026-9184
ABB--Control Builder A	Uncontrolled Search Path Element vulnerability in ABB Control Builder A, ABB 800xA for Advant Master. This issue affects Control Builder A: through 1.4/4; 800xA for Advant Master: through 6.0.3-1, through 6.1.1-1, 6.1.1-3, 6.2.0-1.	2026-06-23	4.4	CVE-2025-13162
About Envato-- BookPro	Unauthenticated Insecure Direct Object References (IDOR) in BookPro <= 1.1.0 versions.	2026-06-26	5.3	CVE-2025-66123
Adobe--Acrobat Reader	Acrobat Reader versions 2020.009.20074, 2020.001.30002, 2017.011.30171, 2015.006.30523 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-23	5.5	CVE-2020-9711
Adobe--Acrobat Reader	Adobe Acrobat and Reader versions 2020.009.20074 and earlier, 2020.001.30002, 2017.011.30171 and earlier, and 2015.006.30523 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-23	5.5	CVE-2020-9713
ailchev-- SearchPlus	The SearchPlus plugin for WordPress is vulnerable to unauthorized modification and deletion of data in versions up to, and including, 1.7.1. This is due to a missing capability check and missing nonce validation on the searchplus_save_token_action_callback() and searchplus_reset_token_action_callback() functions, both of which are exposed to unauthenticated users through the wp_ajax_nopriv_hooks.	2026-06-24	5.3	CVE-2026-8617

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This makes it possible for unauthenticated attackers to overwrite or delete the plugin's stored account token and account name options (dym_token, dym_name, searchplus_token, searchplus_name, sp_token, sp_name).			
ajitdas--Devs Accounting Simple Accounting and Invoicing Solution	The Devs Accounting - Simple Accounting and Invoicing Solution plugin for WordPress is vulnerable to unauthorized modification/deletion of data due to a missing capability check on the delete_single_account() function in versions up to, and including, 1.2.0. The REST route 'devs-accounting/v1/delete-account/(?P<id>\d+)' is registered without any permission_callback, which causes WordPress to expose the endpoint to public, unauthenticated access. This makes it possible for unauthenticated attackers to soft-delete arbitrary accounting account records (wp_dac_accounts) by issuing a simple GET request to the endpoint with any account ID.	2026-06-24	5.3	CVE-2026-9172
ajitdas--Devs Accounting Simple Accounting and Invoicing Solution	The Devs Accounting - Simple Accounting and Invoicing Solution plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 1.2.0. This is due to the get_single_account() REST API callback being registered with a permission_callback that unconditionally returns true, providing no authentication or authorization checks on the /devs-accounting/v1/get-account/<id> endpoint. This makes it possible for unauthenticated attackers to read arbitrary private financial account records (including account name, bank name, and opening balance) by enumerating the numeric account ID, resulting in sensitive information disclosure.	2026-06-24	5.3	CVE-2026-9175
AKIN Software Computer Import Export Industry and Trade Ltd.--e-Commerce	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in AKIN Software Computer Import Export Industry and Trade Ltd. E-Commerce allows Reflected XSS. This issue affects e-Commerce: before 1.25.01.06.	2026-06-23	6.1	CVE-2026-10857
Alps Electric Co., Ltd.--Remote Keyless Entry System (RKES) R53R0	Remote Keyless Entry System (RKES), using the 433 MHz key fob bearing FCC ID CWTR53R0 manufactured by ALPS ALPINE CO., LTD., is vulnerable to a roll-back attack against its rolling-code authentication. An attacker within RF range who records two consecutive lock or unlock transmissions from a legitimate key fob can later replay the same pair of transmissions repeatedly. During testing, replaying the first captured transmission caused the RKES to enter a state in which replaying the second captured transmission resulted in a successful lock or unlock operation of the vehicle. Tested and confirmed on a 2024 Suzuki Swift (SWIFT ISG GLS AC 1.2 5P 4x2 TM).	2026-06-25	6.5	CVE-2026-49319
alsa-project--alsa-lib	The Advanced Linux Sound Architecture (ALSA) library before 1.2.16.1 contains a double-free vulnerability in parse_def() in src/conf.c that allows attackers to corrupt memory by supplying maliciously crafted ALSA configuration text. When parsing nested compound or array configuration blocks, parse_def() fails to check return values before continuing, causing snd_config_delete() to be called twice on the same already-freed node, resulting in a NULL-pointer write or invalid memory read.	2026-06-22	6.8	CVE-2026-56109
antlr--ANTLR4	A security vulnerability has been detected in antlr ANTLR4 up to 4.13.2. Affected by this vulnerability is the function GoTarget of the file tool/src/org/antlr/v4/codegen/target/GoTarget.java of the component	2026-06-28	5.3	CVE-2026-13501

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	gofmt. The manipulation leads to command injection. The attack can only be performed from a local environment. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.			
antlr--ANTLR4	A vulnerability was detected in antlr ANTLR4 up to 4.13.2. Affected by this issue is the function getImportedVocabFile of the file tool/src/org/antlr/v4/parse/TokenVocabParser.java of the component tokenVocab Grammar Option Handler. The manipulation results in path traversal. The attack can be executed remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-28	5.3	CVE-2026-13503
antlr--ANTLR4	A flaw has been found in antlr ANTLR4 up to 4.13.2. This affects the function ObjectInputStream.readObject of the file antlr4-maven-plugin/src/main/java/org/antlr/mojo/antlr4/GrammarDependencies.java of the component Maven Plugin. This manipulation causes time-of-check time-of-use. The attack is restricted to local execution. A high degree of complexity is needed for the attack. It is indicated that the exploitability is difficult. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-28	4.5	CVE-2026-13502
Arraytics--WPCafe	Subscriber Broken Access Control in WPCafe <= 3.0.14 versions.	2026-06-26	4.3	CVE-2026-57622
ArtifexSoftware--mupdf	MuPDF before 1.27.0-rc1 contains an uncontrolled recursion vulnerability in the EPUB CSS rendering engine that allows remote attackers to cause a denial of service by supplying a maliciously crafted EPUB file with deeply nested HTML elements and inline CSS styles. The function value_from_inheritable_property() in css-apply.c recurses through the CSS property inheritance chain without a depth limit, exhausting the process stack and causing a crash in any application using MuPDF for EPUB rendering.	2026-06-23	6.5	CVE-2025-71382
assistioai--Assistio	The Assistio plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check and missing nonce verification on the assistio_plugin_delete_assistio_settings() function in versions up to, and including, 1.1.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete the plugin's options including the critical 'assistio_bot_oauth_settings' option, which disrupts the plugin's integration with the Assistio bot service.	2026-06-24	4.3	CVE-2026-8614
authlib--authlib	Authlib is a Python library which builds OAuth and OpenID Connect servers. Prior to 1.6.10 and 1.7.1, Authlib's OAuth 2.0 authorization endpoint can be turned into an unauthenticated open redirect when a request uses an unsupported response_type and supplies an attacker-controlled redirect_uri. The vulnerable behavior happens before client lookup and before any redirect URI validation. As a result, an attacker does not need a valid client registration, an authenticated user, or any prior state. A single request to the authorization endpoint is enough to obtain a 302 Location response to an arbitrary attacker-controlled URL. This vulnerability is fixed in 1.6.10 and 1.7.1.	2026-06-22	5.4	CVE-2026-41479

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bdthemes--Live Copy Paste for Elementor	Contributor Broken Access Control in Live Copy Paste for Elementor <= 1.5.3 versions.	2026-06-26	4.3	CVE-2025-63079
perfect--Reviews and Rating Docplanner	The Reviews and Rating - Docplanner plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.1.4. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to trigger outbound scraping of external websites and write scraped review data into the wp_dp_reviews database table, as well as send feature-request emails from the site administrator's email address.	2026-06-24	4.3	CVE-2026-9619
bitwarden--server	Bitwarden Server before 2026.5.0 contains a broken access control vulnerability that allows any authenticated user to access arbitrary organization billing data by supplying an arbitrary organizationId to the PreviewInvoiceController endpoints without membership or authorization checks. Attackers can exploit the missing ManageOrganizationBillingRequirement on the preview invoice endpoints to retrieve Stripe-computed tax totals, subscription status, and billing details derived from any target organization's real customer and subscription data.	2026-06-25	4.3	CVE-2026-57521
BlockArt--Magazine Blocks	Contributor Cross Site Scripting (XSS) in Magazine Blocks <= 1.8.3 versions.	2026-06-26	6.5	CVE-2026-57650
bPlugins--Flash & HTML5 Video	Unauthenticated Broken Access Control in Flash & HTML5 Video <= 2.11.0 versions.	2026-06-26	5.8	CVE-2026-57323
Cacti--cacti	Cacti is an open source performance and fault management framework. Versions 1.2.30 and prior are vulnerable to Open Redirect through a substring check rather than a host check at str_contains(\$referer, CACTI_PATH_URL). When the user's login_opts == '1' (redirect to referer after login), the function used \$_SERVER['HTTP_REFERER'] directly. An attacker could craft a referer such as https://evil.com/cacti/. Where CACTI_PATH_URL is /cacti/, the substring matches and the user is redirected to evil.com after login. The pre-existing validate_redirect_url() helper at lib/html_utility.php performed proper validation but was not invoked from auth_login_redirect(). This issue has been fixed in version 1.2.31.	2026-06-25	6.1	CVE-2026-40080
Cacti--cacti	Cacti is an open source performance and fault management framework. Versions 1.2.30 and prior are vulnerable to Path Traversal through the Report format_file Parameter, causing arbitrary file read. This vulnerability occurs in two stages. In the first stage (stored injection), lib/html_reports.php at line 283 stores \$save['format_file'] = \$post['format_file'] directly into the database without any validation. In the second stage (file read), lib/reports.php at line 667 concatenates CACTI_PATH_FORMATS . '/' . \$format_file, and line 670 then calls file(\$format_file), reading arbitrary files from the filesystem. This issue has been fixed in version 1.2.31.	2026-06-25	6.5	CVE-2026-40084
Cacti--cacti	Cacti is an open source performance and fault management framework. Versions 1.2.30 and prior have missing session_regenerate_id() after login, leading to Session Fixation. session_regenerate_id() is NOT called after successful login. The login flow at auth_login.php:203-207 directly sets	2026-06-25	5.4	CVE-2026-40082

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	\$_SESSION[SESS_USER_ID] without rotating the session ID. The session cookie configuration is otherwise good (httponly=true, samesite=Strict, secure=true for HTTPS at include/global.php:513-537), but these do not prevent session fixation via same-site vectors. This issue has been fixed in version 1.2.31.			
caddyserver--caddy	Caddy is an extensible server platform that uses TLS by default. From 2.4.0 until 2.11.3, the authorization layer and the /config traversal layer do not agree on what object the path refers to. In this case, a path authorized for one config object is accepted, but then resolves to a different config object during traversal. This happens because the authorization layer uses string prefix matching and the /config traversal layer parses array indices numerically using strconv.Atoi(). This vulnerability is fixed in 2.11.3.	2026-06-23	5.4	CVE-2026-45692
caddyserver--caddy	Caddy is an extensible server platform that uses TLS by default. Prior to 2.11.4, Caddy's stripHTML template function cannot reliably remove all HTML tags from input strings. Certain malformed HTML, such as <, can bypass the tag-stripping logic, potentially leaving dangerous content in the output if it is later rendered as HTML. This may allow client-side XSS in cases where untrusted strings are rendered unsafely. This vulnerability is fixed in 2.11.4.	2026-06-23	4.2	CVE-2026-52846
Canonical--LXD	Nil-pointer dereference in CreateCustomVolumeFromBackup in LXD up to version 6.8 and 5.21 on Linux allows an authenticated user with can_create_storage_volumes permissions to cause a denial of service via a specially crafted custom-volume backup tarball that omits the expires_at snapshot field.	2026-06-26	6.5	CVE-2026-9639
Canonical--lxd	In Canonical LXD versions 4.12 through 6.9, a Server-Side Request Forgery (SSRF) vulnerability in the image import functionality allows authenticated users with the can_create_images entitlement to interact with internal network infrastructure via the /images endpoint. When importing an image from a URL source, the LXD daemon fails to validate or restrict outbound destination IP addresses, allowing connections to loopback, RFC1918 private ranges, and cloud metadata endpoints. This enables error-based port scanning and unauthorized interaction with internal HTTP services from the daemon's network position.	2026-06-26	5	CVE-2026-28385
Cap-go--capgo	Cap-go before 12.128.2 contains multiple SQL injection vulnerabilities in cloudflare.ts where user-controlled values from API request bodies are interpolated directly into SQL query strings without sanitization or parameterization. Authenticated users with read-level API key permissions can inject arbitrary SQL through devicelds, search, version_name, cursor, and actions parameters to access analytics data belonging to other users or applications.	2026-06-22	6.5	CVE-2026-56221
Cap-go--capgo	Cap-go before 12.128.2 contains an authorization bypass vulnerability in the GET /organization/members endpoint that allows org-limited API keys to bypass limited_to_orgs restrictions. Attackers with org-limited API keys can read membership data including uid, email, image_url, role, and is_tmp from organizations outside their assigned scope.	2026-06-24	4.3	CVE-2026-56310
Capgo--Capgo	Capgo before 12.128.2 contains an unsecured images bucket lacking any row level security controls, allowing unauthenticated attackers to read,	2026-06-24	6.5	CVE-2026-56302

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	insert, and delete stored app icons. Remote attackers can exploit this misconfiguration to delete all icons and leak sensitive app IDs and user IDs.			
Capgo--Capgo	Capgo before 12.128.2 contains a weak parsing vulnerability in the x-limited-key-id header that allows attackers to bypass subkey enforcement by submitting malformed values, zero, or duplicate headers that result in NaN or falsy values. Remote attackers can manipulate the x-limited-key-id header to disable limited key scoping and execute requests using the main API key context instead of restricted subkey permissions.	2026-06-22	6.4	CVE-2026-56306
Capgo--Capgo	Capgo before 12.128.2 contains a credential validation vulnerability in the POST /functions/v1/private/validate_password_compliance endpoint that is callable using only the public Supabase key without authentication. The endpoint is CORS-permissive with wildcard origin allowance and lacks rate limiting, enabling attackers to perform password spraying and credential stuffing attacks to compromise user accounts.	2026-06-23	5.3	CVE-2026-56234
Capgo--Capgo	Capgo before 12.128.2 contains an authorization bypass vulnerability in the public.get_current_plan_max_org RPC function that allows unauthenticated attackers to retrieve arbitrary organization plan limits. Attackers can call the RPC endpoint with any organization UUID using only the public Supabase key to disclose billing information including MAU, bandwidth, storage, and build time limits for any organization.	2026-06-22	5.3	CVE-2026-56311
Capgo--Capgo	Capgo (backend Supabase edge functions) before 12.128.2 does not apply the global authentication middleware to the GET /private/role_bindings/:org_id endpoint, unlike the POST and DELETE role_bindings routes, so unauthenticated requests reach the handler instead of being rejected at the middleware layer. The handler still performs its own authorization check and returns Unauthorized, so no direct data exposure occurs; the flaw is inconsistent authentication enforcement across HTTP methods that could enable authorization bypass if the handler logic changes.	2026-06-22	5.3	CVE-2026-56321
Capgo--Capgo	Capgo before 12.128.2 contains an information disclosure vulnerability in the public.exist_app_v2 RPC function that allows unauthenticated attackers to enumerate app_ids by calling POST /rest/v1/rpc/exists_app_v2 with arbitrary appid parameters. Remote attackers can exploit this SECURITY DEFINER function to determine whether specific app_ids exist in the public.apps table, enabling cross-tenant app enumeration and privacy violations.	2026-06-24	5.3	CVE-2026-56337
Capgo--Capgo	Capgo before 12.128.2 contains a denial of service vulnerability in the /auth/v1/otp endpoint that prevents email verification for two-factor authentication due to captcha validation failures. Authenticated users cannot complete 2FA enrollment as the backend consistently returns HTTP 500 errors with captcha verification process failed messages, blocking access to security controls.	2026-06-24	5.3	CVE-2026-56338
Capgo--Capgo	Capgo before 12.128.2 contains a denial of service vulnerability in the POST /app/demo endpoint that allows authenticated users with org write permissions to create unlimited demo applications without rate limiting or quota enforcement. Attackers can repeatedly invoke this endpoint to generate approximately 138 database write operations per request,	2026-06-22	4.3	CVE-2026-56255

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	causing degraded performance, increased costs, and potential service instability.			
Chris Carlevato--utm.codes	Subscriber Server Side Request Forgery (SSRF) in utm.codes <= 1.9.0 versions.	2026-06-26	6.4	CVE-2026-56026
ChromeDevTools--chrome-devtools-mcp	Chrome DevTools for agents (chrome-devtools-mcp) lets your coding agent control and inspect a live Chrome browser. From 0.20.0 until 1.1.0, The chrome-devtools-mcp daemon writes its PID file with fs.writeFileSync() to a deterministic runtime path. On typical macOS environments, and on Linux sessions where \$XDG_RUNTIME_DIR is unset, that runtime path falls back to /tmp/chrome-devtools-mcp-<uid>/daemon.pid. Because the write does not use O_NOFOLLOW, a local low-privilege user on the same POSIX host can pre-create /tmp/chrome-devtools-mcp-<victim_uid>/daemon.pid as a symlink to a file writable by the victim. When the victim later starts daemon mode, fs.writeFileSync() follows the symlink and truncates the target file to the daemon PID string. This vulnerability is fixed in 1.1.0.	2026-06-24	6.1	CVE-2026-53765
ChromeDevTools--chrome-devtools-mcp	Chrome DevTools for agents (chrome-devtools-mcp) lets your coding agent control and inspect a live Chrome browser. From 0.24.0 until 1.1.0, McpContext.validatePath() enforces workspace roots by checking whether path.resolve(filePath) textually falls under one of the configured root paths. path.resolve() does not canonicalize symbolic links. As a result, a symlink inside a configured workspace root can point to a file outside that root, pass validation, and then be followed by downstream file read/write operations. This bypass applies even when the MCP client correctly declares the roots capability with a non-empty list. It is separate from the documented legacy behavior where missing roots capability allows all paths. The practical impact is a workspace-boundary bypass. In the write direction, filePath-writing tools can overwrite out-of-root files through an in-root symlink. In the read direction, upload_file can read through the symlink and send the file to the currently selected web page. This vulnerability is fixed in 1.1.0.	2026-06-24	6.1	CVE-2026-53766
chuhpl--Book a Room Event Calendar	The Book a Room Event Calendar plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.9. This is due to missing or incorrect nonce validation on the settings_form()/update_settings() functionality. The plugin's options page handler dispatches on the 'action' POST parameter and calls update_settings(), which persists plugin configuration (including the external database host, username, password, prefix, database name, encryption key, and registration page URL) via update_option(), without ever generating a nonce field in the settings form or verifying one (no wp_nonce_field(), check_admin_referer(), or wp_verify_nonce() exists anywhere in the plugin). This makes it possible for unauthenticated attackers to modify the plugin's database connection settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-24	4.3	CVE-2026-9721
Code Amp--Forget About Shortcode Buttons	Contributor Broken Access Control in Forget About Shortcode Buttons <= 2.1.3 versions.	2026-06-26	5.4	CVE-2025-63041

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
codepeople-- CodePeople Post Map for Google Maps	The CodePeople Post Map for Google Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'cpm_point' Post Meta in all versions up to, and including, 1.2.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-27	6.4	CVE-2026-13335
Contempoinc-- Real Estate 7	Unauthenticated Cross Site Request Forgery (CSRF) in Real Estate 7 <= 3.5.9 versions.	2026-06-26	6.5	CVE-2026-57641
Crawl4AI-- Crawl4AI	Crawl4AI before 0.8.7 contains an authentication bypass vulnerability in the monitor router endpoints that allows unauthenticated attackers to access destructive operations. Remote attackers can invoke the /monitor/actions/cleanup endpoint and manipulate monitoring state without authentication, causing service disruption.	2026-06-24	6.5	CVE-2026-56262
Crawl4AI-- Crawl4AI	Crawl4AI before 0.8.7 contains a stored cross-site scripting vulnerability in the monitor dashboard that renders crawl URLs and error messages via innerHTML without escaping. An attacker can submit a crafted crawl request with malicious markup that executes in an operator's browser when viewing the dashboard.	2026-06-23	6.1	CVE-2026-56263
Creative Themes--Blocksy Companion Pro	Unauthenticated Insecure Direct Object References (IDOR) in Blocksy Companion Pro <= 2.1.46 versions.	2026-06-26	5.3	CVE-2026-57630
CridioStudio-- ListingPro	Subscriber Cross Site Scripting (XSS) in ListingPro <= 2.9.11 versions.	2026-06-26	6.5	CVE-2026-56046
danny-avila-- LibreChat	LibreChat is an enhanced ChatGPT clone that supports multiple AI providers. Prior to 0.8.4-rc1, the fix for CVE-2024-11171 (commit bb58a2d0) added limits: { fileSize } to createMultipartInstance() in the file upload routes. However, the POST /api/convo/import endpoint uses a separate multer instance that was never updated with the same limits configuration. Combined with the application-level size check being disabled by default (the CONVERSATION_IMPORT_MAX_FILE_SIZE_BYTES env var is commented out in .env.example), an authenticated user can upload arbitrarily large files to exhaust server disk space and memory. This vulnerability is fixed in 0.8.4-rc1.	2026-06-25	6.5	CVE-2026-54024
danny-avila-- LibreChat	LibreChat is an enhanced ChatGPT clone that supports multiple AI providers. Prior to 0.8.4-rc1, the POST /api/files/images endpoint allows any authenticated user to upload files into any agent's tool_resources (e.g., context, execute_code) without verifying ownership or EDIT permission on the target agent. A permission check was added to the POST /api/files route in a previous patch, but the image upload route was never updated with the same check. An attacker can simply use the image endpoint instead of the file endpoint to bypass the authorization entirely. This vulnerability is fixed in 0.8.4-rc1.	2026-06-25	6.5	CVE-2026-54027
danny-avila-- LibreChat	LibreChat is an enhanced ChatGPT clone that supports multiple AI providers. Prior to 0.8.4-rc1, the fix for CVE-2025-7105 added forkLimiter and forkUserLimiter rate limiters to POST /api/convo/fork to prevent rapid-fire conversation duplication. However, the POST /api/convo/duplicate endpoint - which is in the same file and performs the exact same expensive database operations - was not given any rate	2026-06-25	6.5	CVE-2026-54037

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	limiter. An authenticated user can bypass the CVE-2025-7105 fix by using /duplicate instead of /fork to exhaust server resources. This vulnerability is fixed in 0.8.4-rc1.			
danny-avila-- LibreChat	LibreChat is an enhanced ChatGPT clone that supports multiple AI providers. Prior to 0.8.4-rc1, there is a vulnerability in LibreChat's markdown artifact preview pipeline. The marked library v15.0.12 does not HTML-escape double-quote characters in image alt text when a custom renderer falls through to the default renderer. LibreChat's generateMarkdownHtml function (in client/src/utis/markdown.ts) installs a custom image renderer that returns false for URLs passing the isSafeUrl allowlist check, which causes marked to fall back to its built-in renderer. That built-in renderer inserts the raw alt text into the alt="..." attribute without escaping double-quote characters. An attacker can craft an alt text such as " onload="payload to break out of the attribute and inject an arbitrary event handler. The resulting HTML is then assigned to document.getElementById('content').innerHTML inside the Sandpack preview iframe, causing the payload to execute in the victim's browser. This vulnerability is fixed in 0.8.4-rc1.	2026-06-25	5.4	CVE-2026-54025
danny-avila-- LibreChat	LibreChat is an enhanced ChatGPT clone that supports multiple AI providers. Prior to 0.8.4-rc1, the DELETE /api/messages/:conversationId/:messageId endpoint allows any authenticated user to delete any other user's messages. The validateMessageReq middleware only validates that the conversationId belongs to the requesting user, but the handler calls deleteMessages({ messageId }) using only the messageId as the MongoDB filter - without adding a user constraint. An attacker provides their own valid conversationId (to pass validation) and the victim's messageId (to target deletion), resulting in permanent, irrecoverable message deletion. This vulnerability is fixed in 0.8.4-rc1.	2026-06-25	5.3	CVE-2026-54029
danny-avila-- LibreChat	LibreChat is an enhanced ChatGPT clone that supports multiple AI providers. Prior to 0.8.4-rc1, the GET /api/auth/2fa/enable endpoint can be called by an authenticated user (or attacker with a stolen session) even when 2FA is already fully enabled on the account. This endpoint overwrites the existing TOTP secret, generates new backup codes, and sets twoFactorEnabled to false - all without requiring any TOTP or backup code verification. An attacker with a valid session token can completely take over a victim's 2FA, locking the legitimate user out of their own two-factor authentication. This vulnerability is fixed in 0.8.4-rc1.	2026-06-25	5.3	CVE-2026-54036
danny-avila-- LibreChat	LibreChat is an enhanced ChatGPT clone that supports multiple AI providers. Prior to 0.8.4-rc1, the POST /api/auth/2fa/backup/regenerate endpoint regenerates all 2FA backup codes without requiring any TOTP token or existing backup code verification. An attacker with a stolen session token can silently replace a victim's backup codes and use them to bypass 2FA login or disable 2FA entirely. This vulnerability is fixed in 0.8.4-rc1.	2026-06-25	5.9	CVE-2026-54040
Databend-- Databend	A vulnerability was identified in Databend up to 1.2.881 on HTTP. This affects the function ClientSessionManager::state_key of the file src/query/service/src/servers/http/v1/session/client_session_manager.rs of the component Tenant Handler. The manipulation leads to authorization bypass. It is possible to initiate the attack remotely. The	2026-06-28	6.3	CVE-2026-13512

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploit is publicly available and might be used. The pull request to fix this issue awaits acceptance.			
daytonaio--daytona	Daytona is a secure and elastic infrastructure runtime for AI-generated code execution and agent workflows. Prior to 0.185.0, a cross-tenant authorization flaw in Daytona's notification WebSocket gateway allowed any authenticated user to subscribe to another organization's realtime notification channel and passively receive that organization's events. This vulnerability is fixed in 0.185.0.	2026-06-23	6.5	CVE-2026-54324
daytonaio--daytona	Daytona is a secure and elastic infrastructure runtime for AI-generated code execution and agent workflows. Prior to 0.185.0, the daemon's git clone implementation disabled TLS certificate verification. When a clone request carried Git credentials, the daemon sent the HTTP Basic Authorization header to the remote over a connection whose certificate was never validated, on both the go-git and native git CLI code paths. An attacker able to intercept clone traffic could present any TLS certificate, capture the Git credentials supplied for the clone, and serve tampered repository content into the sandbox. This vulnerability is fixed in 0.185.0.	2026-06-23	5.9	CVE-2026-54323
daytonaio--daytona	Daytona is a secure and elastic infrastructure runtime for AI-generated code execution and agent workflows. Prior to 0.186, a sandbox volume reference (volumeld, which may also be a volume name) was forwarded to the runner and used to build the host bind-mount source path without confinement. A reference containing path-traversal sequences could in principle resolve the mount source outside the intended per-volume base directory. This vulnerability is fixed in 0.186.	2026-06-23	4.2	CVE-2026-54319
Dell--Display and Peripheral Manager	Dell Display and Peripheral Manager (DDPM Mac), versions prior to 2.3, contain a Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') vulnerability. A low-privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of Privileges.	2026-06-25	6.7	CVE-2026-46732
Dell--Wyse Management Suite (WMS)	Dell Wyse Management Suite (WMS), versions prior to WMS 2605, contain a Use of Default Credentials vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information Disclosure.	2026-06-22	6	CVE-2026-44273
denoland--deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.8.0, the Node.js compatibility TCP path checked the permission against the original hostname string before resolution and then did not re-check after resolution. A caller could therefore pass a numeric alias of an IP address (for example the decimal integer 2130706433 or the hex form 0x7f000001, both of which resolve to 127.0.0.1) and reach the denied destination through node:net.connect or node:http.request's { host, port } options form. This vulnerability is fixed in 2.8.0.	2026-06-23	6.5	CVE-2026-49411
denoland--deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.7.12, when Deno was run in BYONM mode (nodeModulesDir: "manual"), the module resolver did not validate that a package's resolved entrypoint stayed within its node_modules/<pkg>/ directory. A malicious package.json whose main field contained .. segments was able to resolve to an arbitrary path on disk, and the resolver then read that file without consulting the --allow-read allowlist. This let a require("evil-pkg") call	2026-06-23	5.5	CVE-2026-49406

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	return the contents of a file that a direct <code>Deno.readFileSync(...)</code> call would have been blocked from reading. This vulnerability is fixed in 2.7.12.			
denoland--deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.8.1, when <code>fetch()</code> was called, Deno checked the destination hostname against <code>--deny-net</code> rules but did not re-check the IP addresses that hostname resolved to. An attacker-controlled script could use a specially crafted domain name that passes the hostname check yet resolves to a denied IP, bypassing the network restriction entirely. This vulnerability is fixed in 2.8.1.	2026-06-23	5.2	CVE-2026-49859
denoland--deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.8.1, when a WebSocket connection was opened, Deno checked the destination hostname against <code>--deny-net</code> rules but did not re-check the IP addresses that hostname resolved to. An attacker-controlled script could use a specially crafted domain name that passes the hostname check yet resolves to a denied IP, bypassing the network restriction entirely. This vulnerability is fixed in 2.8.1.	2026-06-23	5.2	CVE-2026-49860
denoland--deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.8.1, environment access is gated by the <code>env</code> permission. You can deny it with <code>--deny-env</code> , or restrict it to a specific allowlist with <code>--allow-env=FOO,BAR</code> . The expectation is that a program running without <code>env</code> permission cannot change <code>process.env</code> . <code>process.loadEnvFile()</code> (the Node-compatible API for loading variables from a <code>.env</code> file) does not honor this. It only checks that the program has read permission for the <code>dotenv</code> file, then writes every key in that file into the process environment - even when <code>env</code> access is denied. In effect, <code>--allow-read</code> plus a writable or attacker-controlled <code>.env</code> file is enough to defeat <code>--deny-env</code> . This vulnerability is fixed in 2.8.1.	2026-06-23	5.2	CVE-2026-49983
denoland--deno	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Prior to 2.7.5, a Deno program that opens a client WebSocket connection could be crashed by the remote server. While handling the WebSocket handshake response, Deno parsed the <code>Sec-WebSocket-Protocol</code> and <code>Sec-WebSocket-Extensions</code> response headers in a way that assumed their bytes were always printable ASCII. A response header containing non-visible-ASCII bytes (0x80-0xFF) caused a panic that aborted the entire Deno process. This vulnerability is fixed in 2.7.5.	2026-06-23	4.3	CVE-2026-55517
Digiwin--EasyFlow .NET	EasyFlow .NET developed by Digiwin has a Stored Cross-Site Scripting vulnerability, allowing authenticated remote attackers to inject persistent JavaScript code executed in users' browsers upon page load.	2026-06-22	5.4	CVE-2026-12580
docling-project--docling	Docling simplifies document processing by parsing diverse formats and providing integrations with the generative AI ecosystem. From 2.45.0 until 2.91.0, the METS-GBS backend's XML parsing and the input document format detection lacked security controls. An attacker could craft malicious METS-GBS archives that, when processed, could read sensitive files, exhaust system resources, or cause application crashes. This vulnerability is fixed in 2.91.0.	2026-06-26	5.5	CVE-2026-44018
docling-project--docling	Docling simplifies document processing by parsing diverse formats and providing integrations with the generative AI ecosystem. From 2.73.0 until 2.91.0, the LaTeX backend's handling of <code>\includegraphics</code> , <code>\input</code> , and <code>\include</code> commands lacked path containment validation. Attackers could craft malicious LaTeX documents with path traversal sequences to read	2026-06-24	5.5	CVE-2026-44022

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary files from the file system accessible to the process, include sensitive files in the converted document output, or potentially access configuration files, credentials, or other sensitive data This vulnerability is fixed in 2.91.0.			
dokaninc-- Dokan: AI Powered WooCommerce Multivendor Marketplace Solution Build Your Own Amazon, eBay, Etsy	The Dokan: AI Powered WooCommerce Multivendor Marketplace Solution - Build Your Own Amazon, eBay, Etsy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Product SKU in all versions up to, and including, 5.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with custom-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The malicious payload is delivered to site visitors - including unauthenticated users - when the store search widget inserts the unescaped AJAX response HTML into the DOM via jQuery's .html() method.	2026-06-27	6.4	CVE-2026-11783
dokaninc-- Dokan: AI Powered WooCommerce Multivendor Marketplace Solution Build Your Own Amazon, eBay, Etsy	The Dokan: AI Powered WooCommerce Multivendor Marketplace Solution - Build Your Own Amazon, eBay, Etsy plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.0.4 via the 'id' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to read any other vendor's products - including unpublished draft and pending listings - exposing product names, prices, SKUs, and descriptions belonging to other vendors. The permission callbacks for both the collection endpoint and the single-item endpoint only verify the generic vendor capability ('dokan_view_product_menu' / 'dokandar'), which every vendor holds, rather than confirming the requested author ID or product ownership matches the authenticated user.	2026-06-27	4.3	CVE-2026-11987
dokku--dokku	Dokku is a docker-powered PaaS. Prior to 0.38.2, the git:auth command creates \$DOKKU_ROOT/.netrc using bash's touch command, which applies the default umask of 0644. This pre-creation defeats the netrc binary's built-in 0600 permission setting, leaving git credentials readable by any local user who can traverse the dokku home directory. This vulnerability is fixed in 0.38.2.	2026-06-26	5	CVE-2026-45407
dornaweb-- Product Specifications for Woocommerce	The Product Specifications for WooCommerce plugin for WordPress is vulnerable to unauthorized modification, creation, and deletion of data in versions up to and including 0.8.9. This is due to a missing capability check and missing nonce verification in the __invoke() methods of the AttributeGroupController and AttributeController classes, which are bound to the 'dwps_modify_groups' and 'dwps_modify_attributes' AJAX actions. This makes it possible for authenticated attackers, with Subscriber-level access and above, to create, edit, and delete arbitrary product specification groups and attributes (taxonomy terms in the 'spec-group' and attribute taxonomies), corrupting business data and impacting the site's frontend display.	2026-06-27	4.3	CVE-2026-11364
Dynabook Inc.-- Generic IO & Memory Access driver	Generic IO & Memory Access driver for PCs provided by TOSHIBA CORPORATION and Dynabook Inc. exposes its IOCTL with insufficient access control. A logged-in user with no administrative privilege may access physical memory.	2026-06-25	5.5	CVE-2026-56129

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
eamendil-works--pi	Pi is a minimal terminal coding harness. Pi before 0.79.0 loaded project-local configuration and resources from a repository's .pi directory without first asking the user to trust that repository. This included project-local extensions, which are executable TypeScript or JavaScript modules loaded into the Pi process. An attacker who controls a repository could place Pi-specific project resources in that repository. If a user then started Pi from that working tree, the project-local extension code could run with the same privileges as the local Pi process without the user having a convenient way to make a trust decision. This vulnerability is fixed in 0.79.0.	2026-06-23	4.4	CVE-2026-54325
Eclipse Foundation--Eclipse Open VSX	Open VSX Registry does not sanitize SVG files uploaded as extension icons prior to storage, and serves them with Content-Type: image/svg+xml without security headers such as Content-Security-Policy or Content-Disposition: attachment. This allows an attacker to publish an extension with a malicious SVG icon and achieve stored cross-site scripting (XSS) when a user navigates directly to the icon URL. On deployments using local storage, script execution occurs within the Open VSX application origin, enabling session hijacking, authentication token theft, and unauthorized extension publishing. On deployments backed by external storage (such as open-vsx.org with an S3-backed CDN), execution is confined to the storage origin, reducing impact but still permitting phishing attacks and credential harvesting through attacker-crafted pages.	2026-06-23	4.1	CVE-2026-4983
Elementor--Elementor Website Builder	Contributor Sensitive Data Exposure in Elementor Website Builder <= 4.1.3 versions.	2026-06-25	6.5	CVE-2026-57619
eLightUp--Slim SEO	Contributor Broken Access Control in Slim SEO <= 4.6.2 versions.	2026-06-25	6.5	CVE-2026-57429
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. From 1.26.0 until 1.35.13, 1.36.9, 1.37.5, and 1.38.3, the envoy.filters.http.grpc_stats filter crashes (null pointer dereference / segfault) when a Connect protocol request (Content-Type: application/connect+proto or application/connect+json) hits a direct_response route. A single unauthenticated HTTP request crashes the Envoy process. This vulnerability is fixed in 1.35.13, 1.36.9, 1.37.5, and 1.38.3.	2026-06-26	6.5	CVE-2026-47204
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. From 1.34.0 until 1.35.13, 1.36.9, 1.37.5, and 1.38.3, Envoy crashes if an ext_proc server sends a single gRPC message containing multiple, specially crafted ProcessingResponse messages. This can occur when the first response in the batch causes the gRPC stream object to be destroyed, leading to a use-after-free error when Envoy attempts to process subsequent responses in the same gRPC message. This vulnerability is fixed in 1.35.13, 1.36.9, 1.37.5, and 1.38.3.	2026-06-26	6.5	CVE-2026-47207
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to 1.35.11, 1.36.7, 1.37.3, and 1.38.1, the OAuth2 HTTP filter's encrypt()/decrypt() functions use AES-256-CBC without an authentication tag (no HMAC, no AEAD). The /callback endpoint returns HTTP 302 on successful decryption and HTTP 401 on padding failure, creating a padding oracle. An attacker who obtains the encrypted	2026-06-26	6.8	CVE-2026-47775

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	CodeVerifier cookie can recover the plaintext PKCE code_verifier in ~6,200 requests (~100 seconds), then exchange it with a stolen authorization code to obtain the victim's access token. This vulnerability is fixed in 1.35.11, 1.36.7, 1.37.3, and 1.38.1.			
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. From 1.36.0 until 1.36.9, 1.37.5, and 1.38.3, a Use-After-Free (UAF) vulnerability leading to a sudden segmentation fault exists in Envoy's ext_authz HTTP filter when processing per-route authorization overrides concurrently with rapid downstream client disconnects. During standard request lifecycles, Envoy instantiates the ext_authz filter with a foundational authorization client object (client_). If a matched route dictates a dynamic per-route HTTP or gRPC authorization service override, the filter generates a localized client. In the vulnerable implementation, this transient client aggressively overwrote the default client_unique pointer by executing client_ = std::move(per_route_client). When a client rapidly establishes and subsequently tears down a stream (such as rapidly refreshing a protected WebSocket endpoint), the downstream triggers the ConnectionManagerImpl::doDeferredStreamDestroy() -> ActiveStream::onResetStream() lifecycle. Envoy immediately sequences Filter::onDestroy() in an attempt to securely abort dispatched asynchronous authorization check transactions via client_->cancel(). By destructing the default client abruptly during initiateCall, a memory lifecycle misalignment occurs within the async client manager. The stream teardown fails to reliably track and cancel the dynamically bound asynchronous authorization tasks, orchestrating a sequence where a late asynchronous callback from the network evaluates against a heavily destroyed ActiveStream validation span, generating a UAF process crash. This vulnerability is fixed in 1.36.9, 1.37.5, and 1.38.3.	2026-06-26	5.9	CVE-2026-47205
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. From 1.18.0 until 1.35.13, 1.36.9, 1.37.5, and 1.38.3, the router filter contains a null pointer dereference vulnerability when handling HTTP 303 (See Other) internal redirects for body-less non-GET/HEAD requests. When a POST, PUT, DELETE, or PATCH request without a body is sent to a route configured with internal redirect policy that includes 303 in redirect_response_codes, and the upstream responds with HTTP 303, the redirect handling code attempts to drain a request body buffer that was never allocated. This results in a segmentation fault that crashes the entire Envoy process. When route configured with internal_redirect_policy including 303 in redirect_response_codes and upstream must return HTTP 303 response, an unauthenticated attacker can exploit this to cause complete denial of service, terminating all active connections. This vulnerability is fixed in 1.35.13, 1.36.9, 1.37.5, and 1.38.3.	2026-06-26	5.9	CVE-2026-47221
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. From 1.37.0 until 1.37.5 and 1.38.3, the HTTP OAuth2 filter (envoy.filters.http.oauth2) can leave an in-flight async token exchange attached to a downstream stream that has already been torn down. A late AsyncClient completion can still invoke OAuth2Filter methods that use StreamDecoderFilterCallbacks after that object's lifetime has ended, causing undefined behavior, worker crashes (availability loss), and use-after-free / invalid-vptr failures under AddressSanitizer. This is a memory-	2026-06-26	5.9	CVE-2026-48090

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	safety / lifetime issue in the data plane, not a trivial config bug. Remote code execution is not claimed here; the primary demonstrated impact is DoS via crash and UB; any further impact would be deployment- and allocator-dependent. This vulnerability is fixed in 1.37.5 and 1.38.3.			
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to 1.35.11, 1.36.7, 1.37.3, and 1.38.1, in cases where UDP DNS filter is configured with local resolution containing a name with the length of 255 octets or remote resolution for a name of 255 octets long can complete successfully, a query with such name will result in abnormal process termination. The abnormal process termination is triggered by an invalid runtime precondition that the query name is strictly less than 255 octets, contradicting DNS specification rfc1035#section-2.3.4 that the name can be 255 or less octets. This vulnerability is fixed in 1.35.11, 1.36.7, 1.37.3, and 1.38.1.	2026-06-26	5.9	CVE-2026-48497
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. From 1.34.0 until 1.35.13, 1.36.9, 1.37.5, and 1.38.3, a vulnerability exists in Envoy's TCP StatsD sink (TcpStatsdSink), where the thread-local flusher buffer can be overflowed by exceptionally long statistic names (e.g., >16KiB). During formatting, TcpStatsdSink reserves a single contiguous memory slice of 16KiB (FLUSH_SLICE_SIZE_BYTES). If formatting a single metric exceeds the remaining capacity, the flusher initiates a buffer rotation but incorrectly continues to allocate another fixed 16KiB slice. If an attacker can trigger a statistic name longer than 16KiB-for example, by sending an HTTP or gRPC request with an extremely long request path (:path) that is recorded by the grpc_stats filter configured with stats_for_all_methods: true-the flusher will attempt to copy the metric name using memcpy operations beyond the allocated heap buffer boundaries. This leads to a heap write overflow, which can cause immediate denial-of-service (process crash) or potential remote code execution (RCE). This vulnerability is fixed in 1.35.13, 1.36.9, 1.37.5, and 1.38.3.	2026-06-26	5.9	CVE-2026-48706
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. From 1.34.0 until 1.35.13, 1.36.9, 1.37.5, and 1.38.3, PROXY Protocol v2 header generator emits TLVs beyond the maximum length of 65535 bytes, causing a mismatch between bytes written and the length field in the header. This can result in smuggled bytes on the upstream request. This vulnerability is fixed in 1.35.13, 1.36.9, 1.37.5, and 1.38.3.	2026-06-26	4.8	CVE-2026-47692
envoyproxy--envoy	Envoy is an open source edge and service proxy designed for cloud-native applications. Prior to 1.35.11, 1.36.7, 1.37.3, and 1.38.1, a structural flaw was identified in DefaultCertValidator::verifySubjectAltName where the extracted DNS SAN string is cast to a C-style string using .c_str() before being passed to the Utility::dnsNameMatch() algorithm. If the attacker serves a certificate with a dNSName SAN containing an embedded NUL byte, the helper Utility::generalNameAsString captures the complete string including the NUL. However, when .c_str() evaluates it, implicit conversion to absl::string_view inside dnsNameMatch relies on strlen(), prematurely truncating the evaluation context. Envoy evaluates truncated string against the exact required config_san match and returns true, thereby successfully validating the string with the Nul byte for an upstream routing. This vulnerability is fixed in 1.35.11, 1.36.7, 1.37.3, and 1.38.1.	2026-06-26	4.4	CVE-2026-47778

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
EVOKE--EVOKE CSMS	Charging station authentication identifiers are publicly accessible via web-based mapping platforms.	2026-06-25	6.5	CVE-2026-44622
expresstech--Quiz and Survey Master (QSM) Easy Quiz and Survey Maker	The Quiz and Survey Master (QSM) - Easy Quiz and Survey Maker plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 11.1.4. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to create, modify, and delete quiz output templates stored in the mlw_quiz_output_templates database table, including storing unsanitized HTML content such as arbitrary script tags.	2026-06-27	4.3	CVE-2026-9233
fabricjs--fabric.js	Fabric.js is a Javascript HTML5 canvas library. Prior to 7.4.0, a potential Cross-Site Scripting (XSS) vulnerability exists in Fabric.js due to improper escaping of user-controlled input during SVG serialization via the toSVG() method. Specifically, the color field within the colorStops array of a fabric.Gradient object is not properly escaped when converted into SVG <stop> elements. If an application renders the generated SVG string into the DOM, this may allow an attacker to inject arbitrary HTML/SVG and execute JavaScript in the victim's browser. This vulnerability is fixed in 7.4.0.	2026-06-22	5.4	CVE-2026-44311
FasterXML--jackson-databind	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.21.0 until 2.21.4 and 3.1.4, UnwrappedPropertyHandler.processUnwrappedCreatorProperties() replays buffered JSON into creator parameters but never consults prop.visibleInView(activeView). The normal property-based creator path gates creator properties on the active view, but this unwrapped-creator replay path bypasses that check, so a constructor parameter annotated with both @JsonView(AdminView.class) and @JsonUnwrapped is populated from attacker JSON even when a more restrictive view is active. This vulnerability is fixed in 2.21.4 and 3.1.4.	2026-06-23	6.5	CVE-2026-54518
FasterXML--jackson-databind	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.0.0 until 2.18.8, 2.21.4, and 3.1.4, JDKFromStringDeserializer constructed InetAddress with new InetAddress(host, port), which performs eager DNS name resolution for hostname inputs at deserialization time. An application that binds untrusted JSON into a type containing an InetAddress field issues an attacker-chosen DNS query during readValue, before any application-level validation or connect logic. The fix uses InetAddress.createUnresolved(host, port), deferring DNS to an explicit connect. This vulnerability is fixed in 2.18.8, 2.21.4, and 3.1.4.	2026-06-23	5.3	CVE-2026-54514
FasterXML--jackson-databind	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.8.0 until 2.18.9, 2.21.5, and 3.1.4, in BeanDeserializerBase.createContextual(), per-property @JsonIgnoreProperties exclusions are applied by _handleByNameInclusion(), producing a contextual deserializer whose BeanPropertyMap has the ignored properties removed. The subsequent per-property case-insensitivity block (triggered by @JsonFormat(ACCEPT_CASE_INSENSITIVE_PROPERTIES)) rebuilds from this._beanProperties (the original, unfiltered map) instead of contextual._beanProperties, then overwrites the filtered map - restoring every property _handleByNameInclusion had just removed. The ignored	2026-06-23	5.3	CVE-2026-54515

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	property becomes writable again. This vulnerability is fixed in 2.18.9, 2.21.5, and 3.1.4.			
FasterXML-- jackson-databind	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.21.0 until 2.21.4 and 3.1.4, POJOPropertiesCollector._renameProperties() allows a property with @JsonProperty("renamed") on the getter and @JsonIgnore on the setter to be renamed rather than dropped. With MapperFeature.INFER_PROPERTY_MUTATORS enabled (default), the private backing field is retained; during deserialization BeanDeserializerFactory.addBeanProps() sees hasField()==true, builds a FieldProperty, and makes the backing field writable. An attacker supplying the renamed JSON key writes the backing field directly, bypassing the @JsonIgnore on the setter. This vulnerability is fixed in 3.1.4.	2026-06-23	5.3	CVE-2026-54516
FasterXML-- jackson-databind	jackson-databind contains the general-purpose data-binding functionality and tree-model for Jackson Data Processor. From 2.21.0 until 2.21.4 and 3.1.4, in BeanDeserializer._deserializeUsingPropertyBased, the active-view (@JsonView) filter was applied only to creator properties; the regular property-buffering branch performed no prop.visibleInView(activeView) check. A change making SetterlessProperty.isMerging() return true routed setterless Collection/Map properties through this unguarded path, so a setterless collection annotated with a restricted @JsonView is populated from attacker JSON even when the active view excludes it. This vulnerability is fixed in 2.21.4 and 3.1.4.	2026-06-23	5.3	CVE-2026-54517
filamentphp-- filament	Filament is a collection of full-stack components for accelerated Laravel development. From filament/actions 4.0.0 until 4.11.4 and 5.6.4 and from filament/tables 3.0.0 until 3.3.51, the recordSelectOptionsQuery() method may be used to scope the options available in the Select field for AttachAction and AssociateAction. However, the built-in validation rule for these fields did not apply the same scope. As a result, a user who can trigger these actions could tamper with the Livewire component's state and submit an out-of-scope value. This vulnerability is fixed in filament/actions 4.11.4 and 5.6.4 and filament/tables 3.3.51.	2026-06-22	6.5	CVE-2026-48067
filamentphp-- filament	Filament is a collection of full-stack components for accelerated Laravel development. From 4.0.0 until 4.11.5 and 5.6.5, the ImageColumn and ImageEntry components render raw database values without escaping HTML. Where the data passed to these components isn't validated, an attacker could plant malicious HTML or JavaScript and achieve stored XSS that executes for users who view the table or schema. This vulnerability is fixed in 4.11.5 and 5.6.5.	2026-06-22	6.4	CVE-2026-48167
filamentphp-- filament	Filament is a collection of full-stack components for accelerated Laravel development. From 3.0.0 until 3.3.52, 4.11.5, and 5.6.5, any schema can contain a file upload form field, so Filament applies Livewire's WithFileUploads trait to the Livewire component the schema is embedded in. However, some schemas, such as the panel login form, do not require file uploads, and exposing unauthenticated temporary file uploads on these components is not an acceptable risk. On these components, an unauthenticated attacker could upload arbitrary files to the application's temporary storage, which could be abused to exhaust disk space or inflate storage costs. This vulnerability is fixed in 3.3.52, 4.11.5, and 5.6.5.	2026-06-22	6.5	CVE-2026-48500

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
filamentphp--filament	Filament is a collection of full-stack components for accelerated Laravel development. From 4.0.0 until 4.11.5 and 5.6.5, the login page has an observable timing discrepancy that allows unauthenticated attackers to enumerate registered email addresses. The impact is limited to disclosing whether an account exists for a given email. This vulnerability is fixed in 4.11.5 and 5.6.5.	2026-06-22	5.3	CVE-2026-48166
filebrowser--filebrowser	File Browser is a file managing interface for uploading, deleting, previewing, renaming, and editing files within a specified directory. Prior to 2.63.6, unchecked passwords maximums allow for an arbitrarily large password to be passed into the login API. This spikes CPU and memory, and after testing, crashes, heavily lags any container created, and has even made my docker daemon start to send errors with status code 500 even after the container was destroyed. This vulnerability is fixed in 2.63.6.	2026-06-25	6.5	CVE-2026-54092
Flowise--Flowise	Flowise through 2.2.7 contains a SQL injection vulnerability in the importChatflows API. Due to insufficient validation of the chatflow.id value, an authenticated user can supply a crafted JSON import file whose id field is concatenated unsanitized into a SQL IN clause, allowing arbitrary SQL to be executed, including blind and error-based extraction of data from the credential table.	2026-06-24	6.5	CVE-2025-71332
Flowise--Flowise	Flowise before 3.1.3 validates Custom MCP stdio environment variables against a denylist using a case-sensitive comparison, so on Windows, where environment names are case-insensitive, supplying 'node_options' bypasses the NODE_OPTIONS denylist entry. An authenticated user who can configure a Custom MCP node can thereby inject NODE_OPTIONS -- require and execute arbitrary code in the Flowise server context.	2026-06-28	5	CVE-2026-58057
Flowise--Flowise	Flowise before 3.1.0 (npm package flowise, versions 3.0.13 and earlier) uses a weak hardcoded default value 'Secre\$t' for the TOKEN_HASH_SECRET environment variable in packages/server/src/enterprise/utils/tempTokenUtils.ts when the variable is not configured. This secret derives the AES-256-CBC key used to encrypt user IDs and workspace IDs in the 'meta' field of JWT tokens. An attacker who knows the default secret can decrypt this metadata to extract internal user and workspace identifiers, and re-encrypt manipulated values such as altered user or workspace IDs. Because the JWT signature is validated separately, decrypting or tampering with this metadata does not by itself grant access, but the disclosure of internal identifiers and possible metadata manipulation could aid privilege escalation or unauthorized data access.	2026-06-24	4.6	CVE-2026-56269
Flowise--Flowise	Flowise before 3.0.13 uses bcrypt with default salt rounds of 5, providing only 32 iterations instead of the OWASP-recommended minimum of 10 rounds. Attackers can crack password hashes approximately 30 times faster with modern GPU hardware, potentially compromising all user accounts in a database breach scenario.	2026-06-24	4.1	CVE-2026-56272
Fortra--File Integrity Monitoring (FIM)	Fortra File Integrity Monitoring (FIM), formerly Tripwire Enterprise, versions prior to 9.4.0.1 contain a stored cross-site scripting (XSS) vulnerability in the Asset View UI component. An authenticated user with sufficient privileges to create or modify affected node or database configuration fields could store script content that may be rendered as	2026-06-23	5.5	CVE-2026-12163

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	HTML instead of safely escaped text when the affected Asset View UI content is displayed.			
Fortra--File Integrity Monitoring (FIM)	Fortra File Integrity Monitoring (FIM), formerly Tripwire Enterprise, versions prior to 9.4.0 may assign incorrect or elevated effective permissions to users created by the tetool import command while FIM is running, particularly when the import also creates or changes roles or role-permission relationships.	2026-06-23	4.4	CVE-2026-12164
freedesktop.org--libslirp	An out-of-bounds heap read and integer underflow in the TCP urgent data handling (sosendoob) in freedesktop.org libslirp version before v4.9.2 on hypervisor host environments (e.g., QEMU) allows a privileged guest VM attacker (root or CAP_NET_RAW) to leak gigabytes of sensitive host-process heap memory via sending crafted TCP segments with manipulated URG flags and urgent pointers (ti_urp).	2026-06-24	6.5	CVE-2026-9539
FunnelKit--FunnelKit Payment Gateway for Stripe WooCommerce	Unauthenticated Cross Site Request Forgery (CSRF) in FunnelKit Payment Gateway for Stripe WooCommerce <= 1.14.0.3 versions.	2026-06-26	6.5	CVE-2026-57635
Gemini Labs--Site Reviews	Subscriber Sensitive Data Exposure in Site Reviews <= 8.0.11 versions.	2026-06-26	6.5	CVE-2026-57318
GeoVision Inc.--GeoVision	A memory corruption vulnerability exists in the GV-Cloud functionality of GeoVision GV-VMS V20 20.0.2. A specially crafted network request can lead to a denial of service. An attacker can impersonate the legitimate server to trigger this vulnerability.	2026-06-24	6.2	CVE-2026-12488
GhozyLab--Image Carousel	Contributor Cross Site Scripting (XSS) in Image Carousel <= 1.0.0.41 versions.	2026-06-26	6.5	CVE-2025-68074
github--github-mcp-server	GitHub MCP Server is GitHub's official MCP Server. From 0.22.0 until 1.1.2, when running in HTTP mode with --lockdown-mode enabled, the RepoAccessCache is implemented as a process-global singleton initialized with the first authenticated user's GraphQL client. All subsequent requests from different users share this singleton and their lockdown-related GraphQL queries are executed using the first user's credentials. The singleton is never updated to reflect later users' tokens. This vulnerability is fixed in 1.1.2.	2026-06-26	6	CVE-2026-48529
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 13.11 prior to 18.11.6, 19.0 prior to 19.0.3, and 19.1 prior to 19.1.1 in which incorrect authorization in DAST site profile management could allow a user with Developer role to exfiltrate DAST site profile secrets under certain conditions.	2026-06-25	5.3	CVE-2026-11379
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.5 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1 that under certain conditions could have allowed an unauthenticated user to view confidential issue references on public projects due to improper authorization checks.	2026-06-25	5.3	CVE-2026-2238

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 18.6 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1 that under certain conditions could have allowed an authenticated user to read or modify another group's virtual registry cleanup policy settings without authorization.	2026-06-25	5.4	CVE-2026-5309
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 14.8 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1 that under certain conditions could have allowed an authenticated user to conceal content within a Snippet due to improper input validation.	2026-06-25	4.3	CVE-2026-1606
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 13.6 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1 that under certain conditions could have allowed an authenticated user with Reporter-level group permissions to view package metadata from projects with the Package Registry disabled due to incorrect authorization checks in the group packages feature.	2026-06-25	4.3	CVE-2026-5796
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 17.11 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1 that under certain conditions could have allowed an authenticated user with developer-role permissions to bypass package protection rules and overwrite protected Maven package metadata due to incorrect authorization checks.	2026-06-25	4.3	CVE-2026-5952
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 9.3 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1 that under certain conditions could have allowed sensitive information to be written to application logs due to insufficient filtering in a CI/CD API endpoint.	2026-06-25	4.4	CVE-2026-8330
GNU--libidn	GNU libidn before 1.44 is prone to out-of-bounds reads of uninitialized memory in the ToUnicode APIs because of mishandling in idna_to_unicode_internal. The affected code is not present in libidn2.	2026-06-23	4	CVE-2026-57053
gogs--gogs	Gogs is an open source self-hosted Git service. Prior to 0.14.3, password-reset tokens are generated using conf.Auth.ActivateCodeLives (the account-activation lifetime), not conf.Auth.ResetPasswordCodeLives. The token lifetime is baked into the token itself at generation time and is re-extracted from the token at verification time, making RESET_PASSWORD_CODE_LIVES irrelevant to actual enforcement. When an administrator configures a shorter reset window (e.g., 10 minutes) for compliance or security reasons, reset tokens remain exploitable for the full activation lifetime instead, while the reset email falsely advertises the shorter expiry. This vulnerability is fixed in 0.14.3.	2026-06-24	6.8	CVE-2026-52809
gogs--gogs	Gogs is an open source self-hosted Git service. Prior to 0.14.3, an open redirect vulnerability exists in Gogs where attacker-controlled redirect_to parameters can bypass validation, allowing redirection to arbitrary external sites. All redirects in Gogs that are validated via the IsSameSite function are vulnerable. The function only inspects the first two characters of the URL string. This check fails to account for directory traversal sequences followed by backslashes. This vulnerability is fixed in 0.14.3.	2026-06-24	5.4	CVE-2026-52802
gogs--gogs	Gogs is an open source self-hosted Git service. Prior to 0.14.3, a malicious user with rights to create a new file on a repository or wiki page can trigger a denial of service condition in which the pages containing the listing of	2026-06-24	4.9	CVE-2025-64719

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	files will return HTTP error 500 and render the web interface unusable for the repository or wiki. The issue is present in file internal/route/repo/wiki.go and internal/route/repo/view.go where the pages try to recover commit information. If errors are returned while recovering commit information, the page will return a 500 error and stop rendering, resulting in a denial of service. This vulnerability is fixed in 0.14.3.			
gogs--gogs	Gogs is an open source self-hosted Git service. In 0.14.3 and earlier, any authenticated user can watch a private repository they have no access to, because the access check in the Watch API handler is inverted. The code checks if repoCtx.ViewerCanRead() (returns 404 when the user CAN read) instead of if !repoCtx.ViewerCanRead() (return 404 when the user CANNOT read). Once watching, the attacker's dashboard activity feed shows commit messages, branch names, issue titles, and PR details from the private repository. If email notifications are enabled, the attacker also receives emails containing issue and comment content.	2026-06-24	4.3	CVE-2026-52795
gophish--gophish	Gophish through 0.12.1 contains a denial of service vulnerability that allows authenticated users with the User role to exhaust server memory by uploading a crafted Office document as an email template attachment. The ApplyTemplate() function in models/attachment.go processes Office documents as ZIP archives and calls ioutil.ReadAll() on each contained file entry without enforcing size restrictions on uncompressed content, allowing a zip bomb payload to expand to several gigabytes in memory and cause the process to be terminated by the operating system.	2026-06-22	6.5	CVE-2026-39904
gpriday--Page Builder by SiteOrigin	The Page Builder by SiteOrigin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via panels_data Parameter in all versions up to, and including, 2.34.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is possible because the nonce and edit_post capability checks enforced during save are both satisfied by Contributor-level users for their own posts, and the panels_data value is stored as post meta - outside the scope of WordPress's unfiltered_html carve-out - meaning no wp_kses fallback prevents the unsanitized WP_Widget_Custom_HTML content from being persisted and later rendered verbatim on the frontend.	2026-06-27	6.4	CVE-2026-13295
Grafana--Grafana OSS	The Tempo and Loki datasource plugins construct backend HTTP requests by interpolating user-supplied input into URL paths without sanitization, enabling path traversal. A Viewer-role user can: (1) capture admin-configured datasource credentials (secureJsonData custom headers) by traversing to an attacker-controlled endpoint, (2) invoke state-changing admin endpoints on Tempo (e.g. /flush, /shutdown), and (3) exfiltrate internal service data via Loki's CallResource which returns full HTTP response bodies.	2026-06-22	5.4	CVE-2026-10601
Grav--Grav	Grav before 2.0.0-beta.2 contains an XML external entity injection vulnerability in SVG file upload processing that allows authenticated attackers to read arbitrary files. The application uses simplexml_load_string without disabling external entity loading, enabling	2026-06-23	6.5	CVE-2026-56701

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers to inject XXE payloads via malicious SVG files to exfiltrate sensitive data.			
Grav--Grav	Grav before 1.6.30 contains a cross-site scripting vulnerability in the Admin plugin page editor default security configuration. Privileged users with page editing capabilities can inject malicious scripts to execute arbitrary code and install malicious plugins for system access.	2026-06-25	5.4	CVE-2020-37256
GravityKit--GravityView	Unauthenticated Insecure Direct Object References (IDOR) in GravityView <= 3.0.0 versions.	2026-06-26	5.3	CVE-2026-57665
GravityMore--Gravity Bookings	The Gravity Forms Booking plugin for WordPress is vulnerable to time-based SQL Injection via the 'staff_id' parameter in all versions up to, and including, 2.7.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-06-25	6.5	CVE-2026-2508
grokability--snipe-it	Snipe-IT is an IT asset/license management system. In versions prior to 8.6.0, a user with only users.edit can send a PATCH to /api/v1/users/{their_own_id} and grant themselves any permission except admin and superuser - for example 'assets.view', 'assets.create', 'reports.view', import, etc. The issue is patched in version 8.6.0.	2026-06-23	5.5	CVE-2026-48493
guzzle--guzzle	Guzzle is an extensible PHP HTTP client. Prior to 7.12.1, in certain configurations, traffic expected to be protected by TLS on the hop to the proxy is transmitted in cleartext. Proxy authentication credentials (the Proxy-Authorization header, proxy userinfo in the proxy URL, or CURLOPT_PROXYUSERPWD) are sent without encryption, and the CONNECT target host and port for tunneled HTTPS requests are exposed. The built-in cURL handlers (GuzzleHttp\Handler\CurlHandler and GuzzleHttp\Handler\CurlMultiHandler, used by default whenever the PHP cURL extension is available) accept an https:// proxy. libcurl older than 7.50.2 silently treats an https:// proxy as a plaintext http:// proxy. The TLS connection to the proxy is never established, and the proxy leg is cleartext with no error or warning. An application is affected when it sends requests through one of the built-in cURL handlers, configures an https:// proxy expecting the proxy connection itself to be encrypted, and runs with libcurl older than 7.50.2. This vulnerability is fixed in 7.12.1.	2026-06-23	5.9	CVE-2026-55568
guzzle--guzzle	Guzzle is an extensible PHP HTTP client. Prior to 7.12.1, CookieJar incorrectly accepts cookies with a dot-only Domain attribute and whitespace-padded variants. SetCookie::matchesDomain() removes leading dots from the cookie domain, normalizing dot-only values to the empty string; SetCookie::validate() only rejected a strictly empty domain, so these cookies could be stored and the empty normalized domain was treated as matching any request host. An attacker-controlled origin that an application requests with a shared cookie jar can therefore set a cookie that Guzzle later sends to unrelated hosts using the same jar. This may allow cookie injection or session fixation against downstream services, depending on how those services interpret the injected cookie. This vulnerability is fixed in 7.12.1.	2026-06-23	5.8	CVE-2026-55767

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
guzzle--psr7	guzzlehttp/psr7 is a PSR-7 HTTP message library implementation in PHP. Prior to 2.12.1, guzzlehttp/psr7 did not reject CR/LF characters in certain first-party HTTP start-line fields: the request method, protocol version, and response reason phrase. If an application placed attacker-controlled data into one of those fields and later serialized the PSR-7 message as raw HTTP/1.x, for example with Message::toString() or an equivalent serializer, the serialized message could contain attacker-controlled header lines. The issue can also be reached through Message::parseRequest() or Message::parseResponse() when malformed raw messages are parsed into first-party PSR-7 objects and then serialized again. Creating or modifying a Request, Response, or other PSR-7 object alone is not sufficient. The issue requires the malformed message to be serialized and written to the network, forwarded, replayed, or otherwise processed by software that does not independently reject the malformed start line. This vulnerability is fixed in 2.12.1.	2026-06-23	4.8	CVE-2026-55766
halo-dev--halo	Halo is an open source website building tool. Prior to 2.24.3, a path traversal vulnerability in the backup download endpoint allows authenticated administrators to read arbitrary files from the server filesystem. The backup download endpoint (GET /apis/console.api.migration.halo.run/v1alpha1/backups/{name}/files/{filename}) in MigrationServiceImpl.download() resolves the backup filename via Path.resolve() without validating that the resolved path stays within the designated backups directory. Also, the Backup creation endpoint (POST /apis/migration.halo.run/v1alpha1/backups) does not sanitize the status fields during creation This vulnerability is fixed in 2.24.3.	2026-06-25	5.5	CVE-2026-55439
harmonic_design--HD Quiz	The HD Quiz plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions 2.2.0 to 2.2.1. This is due to missing or incorrect nonce validation on the hdq_validate_nonce function. This makes it possible for unauthenticated attackers to delete or modify quizzes and questions, create new quizzes, and change plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-27	4.3	CVE-2026-13422
HCLSoftware--Traveler for Microsoft Outlook	The HCL Traveler for Microsoft Outlook libraries are being flagged as potentially malicious software or an unrecognized application.	2026-06-26	6.7	CVE-2024-23581
HCLSoftware--Traveler for Microsoft Outlook	HCL Traveler for Microsoft Outlook (HTMO) is susceptible to a sensitive data exposure vulnerability which could allow an attacker to exploit application information to then attempt additional attacks and cause unknown behavior in the application.	2026-06-27	5.5	CVE-2025-59868
HKUDS--OpenHarness	OpenHarness ohmo gateway /resume and /summary slash commands default remote_invocable to True, allowing admitted remote senders to enumerate and load arbitrary session snapshots by ID. Attackers can exploit this to access victim snapshots containing private prompts, credentials, tool output, and file paths via shared gateway channels.	2026-06-23	6.5	CVE-2026-56695
HKUDS--OpenHarness	OpenHarness /issue and /pr_comments slash commands lack remote_invocable=False protection, allowing remote channel senders to write attacker-controlled Markdown into project context files. Admitted remote attackers can inject malicious content into .openharness/issue.md	2026-06-23	5.4	CVE-2026-56696

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and .openharness/pr_comments.md files, which are subsequently injected into runtime system prompts, persistently influencing local agent behavior.			
Hono--Hono	Hono before 4.12.12 does not validate cookie names on the write path in the setCookie(), serialize(), and serializeSigned() functions, allowing invalid characters such as control characters (e.g. \r or \n) when an application passes a user-controlled cookie name. This can produce malformed Set-Cookie header values. In modern runtimes such as Node.js and Cloudflare Workers, such invalid header values are rejected and cause a runtime error before the response is sent, so header injection or response splitting could not be reproduced; the issue primarily affects correctness and robustness, resulting in runtime errors (availability) rather than confirmed header injection.	2026-06-23	5.3	CVE-2026-56762
hono--hono	hono before 4.12.14 contains an html injection vulnerability in jsx server-side rendering that allows attackers to inject unintended html by using malformed attribute names. Attackers can craft specially crafted attribute keys containing characters like quotes or angle brackets to break html tag boundaries and inject arbitrary attributes or elements.	2026-06-24	4.3	CVE-2026-56761
honojs--hono	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.25, the Body Limit Middleware trusts the request's Content-Length header to decide whether a body is within the limit. On AWS Lambda (API Gateway v1/v2, ALB, VPC Lattice, and Lambda@Edge) the body is delivered fully buffered and the adapter builds the request with the client-declared Content-Length, which need not match the actual payload. A client can declare a tiny Content-Length while sending a much larger body, slipping past the limit. This vulnerability is fixed in 4.12.25.	2026-06-22	6.5	CVE-2026-54288
honojs--hono	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.25, on Windows hosts, an encoded backslash (%5C) in the request path decodes to \, which the Windows path resolver treats as a separator. serve-static then resolves a single URL segment such as admin\secret.txt into a nested file under the root and serves it, letting an attacker read static files meant to be protected behind prefix-mounted middleware. This vulnerability is fixed in 4.12.25.	2026-06-22	5.9	CVE-2026-54286
honojs--hono	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.25, on AWS Lambda, the ALB single-header response and the VPC Lattice v2 response join multiple Set-Cookie headers into one comma-separated value. Because commas also appear inside cookie attributes (for example Expires dates), clients cannot split the value back into individual cookies and silently drop or misparse them. This vulnerability is fixed in 4.12.25.	2026-06-22	5.3	CVE-2026-54287
honojs--hono	Hono is a Web application framework that provides support for any JavaScript runtime. Prior to 4.12.25, on AWS Lambda@Edge, CloudFront delivers a request header that appears more than once as several separate entries. The adapter writes each value with Headers.set instead of Headers.append, so every value overwrites the previous one and only the last reaches the application. Repeated request headers such as X-Forwarded-For, Forwarded, and Via are silently truncated to a single value. Request middleware sees only the last value of a repeated header instead	2026-06-22	4.8	CVE-2026-54289

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of the full chain. For applications that base access control on the X-Forwarded-For chain, this can weaken or alter that decision; for auditing, hop history is lost. This vulnerability is fixed in 4.12.25.			
iamranit-- Advanced Contact Form 7 Compact DB	The Advanced Contact Form 7 - Compact DB plugin for WordPress is vulnerable to unauthorized deletion of data due to a missing capability check on the cf7cdb_ajax_delete_user() function in versions up to, and including, 1.0.0. The handler is registered against both `wp_ajax_cf7cdb_delete` and `wp_ajax_nopriv_cf7cdb_delete`, and it performs no nonce verification, no capability check, and no ownership check before invoking `\$wpdb->delete()` against the `wp_cf7cdb_data` table with an attacker-supplied integer ID. This makes it possible for unauthenticated attackers to delete arbitrary contact form submission entries stored by the plugin by iterating sequential primary-key IDs.	2026-06-24	5.3	CVE-2026-12094
IBM--Datacap	IBM Datacap 9.1.7, 9.1.8, and 9.1.9 and IBM Datacap Navigator 9.1.7, 9.1.8, and 9.1.9 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-06-22	6.1	CVE-2026-8059
IBM--Datacap	IBM Datacap 9.1.7, 9.1.8, and 9.1.9 and IBM Datacap Navigator 9.1.7, 9.1.8, and 9.1.9 allows an attacker to retrieve user passwords and cryptographic keys from memory. Attacker can use the same keys to decrypt password, gain access to the application and access sensitive data in the database.	2026-06-22	5.5	CVE-2026-8636
IBM--Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data versions 4.8,5.0,5.1,5.2,5.3 could allow an authenticated user to cause a denial of service when creating new databases due to improper allocation of resources.	2026-06-22	6.5	CVE-2024-54178
IBM--Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data versions 4.8, 5.0, 5.1, 5.2, 5.3 could allow a privileged user to perform operations and obtain sensitive information outside of their authority due to improper token validation.	2026-06-22	6	CVE-2025-2669
IBM--Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data versions 4.8, 5.0, 5.1, 5.2, and 5.3 could allow an authenticated user to bypass client-side validation and manipulate input data using man in the middle techniques.	2026-06-22	5.3	CVE-2023-33854
IBM--Engineering Workflow Management	IBM Engineering Workflow Management 7.0.2 through 7.0.2 Interim Fix 035, 7.0.3 through 7.0.3 Interim Fix 017, and 7.1 through 7.1 Interim Fix 004 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking.	2026-06-22	6.5	CVE-2024-51454

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--Engineering Workflow Management	IBM Engineering Workflow Management 7.0.3 through 7.0.3 Interim Fix 020, and 7.1 through 7.1 Interim Fix 007 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-06-22	5.4	CVE-2025-33128
IBM--i	IBM WebSphere Application Server and IBM WebSphere Application Server Liberty are vulnerable to denial of service in the WebSphere WebServer Plug-in component when an attacker can pass crafted requests to the web server.	2026-06-22	5.9	CVE-2026-10852
IBM--IBM Watson Speech Services Cartridge	IBM Watson Speech Services Cartridge is vulnerable to Server-Side Request Forgery (SSRF) in Sterling File Gateway, due to a flaw which may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks [GHSA-rr7j-v2q5-chgv] [CVE-2026-7253]. IBM Sterling File Gateway is used in our speech runtimes. This vulnerability has been addressed. Please read the details for remediation below.	2026-06-22	5.3	CVE-2026-7253
IBM--TRIRIGA Application Platform	IBM TRIRIGA Application Platform 5.0.2 through 5.0.3 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-06-22	5.4	CVE-2026-11372
IBM--WebSphere Application Server	IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.6 are vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources.	2026-06-22	5.9	CVE-2026-9320
itsourcecode--Hospital Management System	A vulnerability was found in itsourcecode Hospital Management System 1.0. The affected element is an unknown function of the file /ajaxmedicine.php. The manipulation of the argument medicineid results in sql injection. It is possible to launch the attack remotely. The exploit has been made public and could be used.	2026-06-28	6.3	CVE-2026-13496
itsourcecode--Hospital Management System	A vulnerability was determined in itsourcecode Hospital Management System 1.0. The impacted element is an unknown function of the file /appointment.php. This manipulation of the argument editid causes sql injection. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2026-06-28	6.3	CVE-2026-13497
itsourcecode--Hospital Management System	A vulnerability has been found in itsourcecode Hospital Management System 1.0. Impacted is an unknown function of the file /adminprofile.php. The manipulation of the argument loginid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2026-06-28	4.7	CVE-2026-13495
jdx--mise	mise manages dev tools like node, python, cmake, and terraform. From 2026.3.15 until 2026.6.4, mise loads github.credential_command from local project config before any trust decision, then executes that value with sh -c when resolving a GitHub token. An attacker who can place a .mise.toml in a repository can execute arbitrary shell commands when the	2026-06-26	6.3	CVE-2026-55448

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	victim runs a GitHub-related mise command and no higher-priority GitHub token environment variable is set. This vulnerability is fixed in 2026.6.4.			
jdx--mise	mise manages dev tools like node, python, cmake, and terraform. Prior to 2026.6.1, the mise HTTP backend builds its install symlink destination from the raw resolved version string for non-latest versions. Normal tool install paths use the sanitized version pathname, but the HTTP backend's symlink path uses the raw value. On Unix-like systems, if that version is an absolute path, PathBuf::join discards the intended mise installs root. A repository-controlled .tool-versions file can therefore make mise install create a symlink outside the mise install tree. With bin_path, the same issue can place an executable symlink under an attacker-selected absolute prefix, such as a developer-tool prefix that is later added to PATH. This vulnerability is fixed in 2026.6.1.	2026-06-26	5.5	CVE-2026-54557
jegstudio--Gutenverse WordPress Blocks, Page Builder & Site Editor	The Gutenverse - WordPress Blocks, Page Builder & Site Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 3.8.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2026-06-27	4.4	CVE-2026-12399
jellyfin--jellyfin	Jellyfin is an open source self hosted media server. Prior to 10.11.9, a potential XSS attack exists in Jellyfin which can allow a non-privileged user to execute arbitrary Javascript in the context of a logged-in Administrative user, resulting in numerous potential issues. The Client header during an AuthenticateByName can contain arbitrary HTML and Javascript, which will then be executed by the Administrative user when visiting the Access tab of the user in question from within the dashboard. This vulnerability is fixed in 10.11.9.	2026-06-24	5.7	CVE-2026-49220
JetBrains--Kotlin	In JetBrains Kotlin before 2.4.20 code execution was possible via unsafe deserialization in the build cache metadata	2026-06-26	6.7	CVE-2026-53914
JetBrains--YouTrack	In JetBrains YouTrack before 2026.2.16593 improper authorisation in the app configurations endpoint allowed modifying project settings	2026-06-26	5.3	CVE-2026-57923
JetBrains--YouTrack	In JetBrains YouTrack before 2026.2.16593 improper access control allowed reading users' private data via the comment templates endpoint	2026-06-26	4.3	CVE-2026-57921
JetBrains--YouTrack	In JetBrains YouTrack before 2026.2.16593 default role configuration exposed excessive user profile details	2026-06-26	4.3	CVE-2026-57924
JetBrains--YouTrack	In JetBrains YouTrack before 2026.2.16593 improper access control allowed reading saved queries and tags	2026-06-26	4.3	CVE-2026-57925
jetmonsters--Restaurant Menu by MotoPress	Subscriber Broken Access Control in Restaurant Menu by MotoPress <= 2.4.11 versions.	2026-06-26	4.3	CVE-2025-63078
JoomSky--JS Help Desk	Unauthenticated Insecure Direct Object References (IDOR) in JS Help Desk <= 3.1.0 versions.	2026-06-26	5.3	CVE-2026-57652

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
joomla--WP Latest Posts	The WP Latest Posts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via crafted image src attributes in post content in versions up to, and including, 5.0.11. This is due to insufficient output escaping in the field() and loop() functions, which extract the raw src attribute value from tags within post_content using a regular expression and then reconstruct new elements or CSS background-image declarations by directly concatenating the unescaped value - bypassing WordPress's kses filtering entirely. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-24	6.4	CVE-2026-9620
joomla--WP Meta SEO	The WP Meta SEO plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 4.5.18 via the 'new_link' parameter. This makes it possible for authenticated attackers, with contributor-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services. The HTTP response status from outbound requests is reflected back in the AJAX JSON response as status_code, providing an enumeration oracle usable for probing internal hosts and cloud metadata services.	2026-06-24	6.4	CVE-2026-11370
jotis--Blue Captcha	The Blue Captcha plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to and including 2.0.1. This is due to missing or incorrect nonce validation on the main admin panel (blcap_main_page) and on the Hall of Shame and Log subpages, which accept a 'blcap_action' / 'action' parameter from \$_REQUEST and perform destructive operations (plugin uninstall via blcap_uninstall(), log deletion via blcap_delete_logs(), Hall of Shame deletion via blcap_delete_ip_db(), and adding IPs to the banned list via update_option('blcap_settings')) with no wp_verify_nonce(), check_admin_referer(), or check_ajax_referer() calls anywhere in the codebase. This makes it possible for unauthenticated attackers to uninstall the plugin, delete audit logs, remove Hall of Shame entries, and add arbitrary IP addresses to the block list via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-24	4.3	CVE-2026-10552
k3s-io--k3s	K3s is a fully conformant production-ready Kubernetes distribution. Prior to 1.35.3+k3s1, 1.34.6+k3s1, v1.33.10+k3s1, a path traversal vulnerability exists in K3s's etcd snapshot decompression functionality. Zip files containing archive members with maliciously crafted names can be written to arbitrary locations on the filesystem when an administrator restores the archive as a compressed etcd snapshot. This vulnerability is fixed in 1.35.3+k3s1, 1.34.6+k3s1, v1.33.10+k3s1.	2026-06-25	5.8	CVE-2026-54250
kanboard--kanboard	Kanboard through 1.2.52, fixed in commit 928c68a, UserController::removeSession fails to validate the session id parameter before passing it to RememberMeSessionModel::remove, allowing authenticated users to delete other users' Remember Me sessions. Attackers can enumerate sequential session IDs and mass-invalidate persistent login sessions of any user, including administrators, forcing re-authentication and causing denial of service.	2026-06-25	5.4	CVE-2026-56774
Kerry--BNE Testimonials	Contributor Cross Site Scripting (XSS) in BNE Testimonials <= 2.0.8 versions.	2026-06-26	6.5	CVE-2025-68075

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kestra-io--kestra	Kestra is an open-source, event-driven orchestration platform. Prior to 1.0.45 and 1.3.21, the previewFileFromExecution endpoint (GET /api/v1/{tenant}/executions/{executionId}/file/preview) contains an access control bypass that allows any authenticated user to read output files from any other execution within the same tenant, bypassing execution-level and namespace-level isolation. This vulnerability is fixed in 1.0.45 and 1.3.21.	2026-06-26	6.5	CVE-2026-53577
khoj-ai--khoj	A flaw has been found in khoj-ai khoj up to 2.0.0-beta.28. This impacts an unknown function of the file src/khoj/routers/api_chat.py of the component Conversation Sharing Handler. This manipulation of the argument conversation.agent causes incorrect authorization. Remote exploitation of the attack is possible. The exploit has been published and may be used. The pull request to fix this issue awaits acceptance.	2026-06-28	5.5	CVE-2026-13508
Knit Pay--UPI QR Code Payment Gateway for WooCommerce	Customer Broken Access Control in UPI QR Code Payment Gateway for WooCommerce <= 1.6.2 versions.	2026-06-25	5.4	CVE-2026-56023
krishaweb--Advance Nav Menu Manager	The Advance Nav Menu Manager plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.3. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to duplicate, copy, move, or publish nav_menu_item posts via wp_insert_post(), modifying the site's navigation menus without authorization.	2026-06-24	4.3	CVE-2026-8688
langchain-ai--langchain	LangChain is a framework for building agents and LLM-powered applications. Prior to 1.3.9, several LangChain components that resolve filesystem paths or expand search patterns do not consistently confine the resolved path to the intended root directory. Affected behaviors include: a file-search agent middleware that validates a starting directory but not the search pattern or the resolved target of matched files, so glob patterns and symlinks can reach files outside the configured root; prompt- and chain/agent-configuration loaders that accept path fields and resolve them without confining the result to a trusted base or rejecting symlink targets; and path-prefix authorization checks that compare by string prefix without a path-segment boundary, so a sibling path sharing the prefix is accepted. When these components receive path values, search patterns, or workspace contents influenced by an untrusted source - including an LLM acting on untrusted input - the result can be disclosure of files outside the intended boundary. This vulnerability is fixed in 1.3.9.	2026-06-22	5.1	CVE-2026-55443
langflow-ai--langflow	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.9.0, Langflow is vulnerable to Path Traversal in the Knowledge Bases API (POST /api/v1/knowledge_bases). This occurs because user-supplied knowledge base names are used directly to create file paths without proper sanitization or containment checks. An authenticated attacker can exploit this flaw to create directories and write files anywhere on the server's filesystem. This vulnerability is fixed in 1.9.0.	2026-06-23	6.5	CVE-2026-42867
langflow-ai--langflow	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.10.0, the "Shareable Playground" (or "Public Flows" in code) contains a potential arbitrary file-read vulnerability, depending on	2026-06-23	6.1	CVE-2026-48520

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the exact flow configuration used. By making a flow public, public execution of the flow is allowed. The execution request can contain a list of files that gets read by Langflow and fed into the LLM. The files path can be any path supported by the storage - it can be either a local file or S3 path if supported by the local configuration This vulnerability is fixed in 1.10.0.			
langflow-ai--langflow	Langflow is a tool for building and deploying AI-powered agents and workflows. Prior to 1.7.0, the logout button does not clear the session. The previous user stays logged in unless another user explicitly logs in. This vulnerability is fixed in 1.7.0.	2026-06-23	6.1	CVE-2026-55423
libssh2--libssh2	libssh2 through 1.11.1 grows its pubkey list with SSH2_REALLOC but does not zero-initialize new entries before parsing populates them, so a parse failure reaching the cleanup path leaves libssh2_pubkey_list_free operating on an uninitialized entry. A malicious SSH server offering the pubkey subsystem can use a malformed response to make cleanup free an uninitialized, attacker-influenceable attrs pointer in a connecting libssh2 client.	2026-06-28	6.5	CVE-2026-58051
magepeopleteam--Booking and Rental Manager	Unauthenticated Broken Access Control in Booking and Rental Manager <= 2.7.1 versions.	2026-06-26	5.3	CVE-2026-57660
Majestic Support--Majestic Support	Subscriber Insecure Direct Object References (IDOR) in Majestic Support <= 1.1.7 versions.	2026-06-26	5.4	CVE-2026-57646
manuelpadillac--MP Customize Login Page	The MP Customize Login Page plugin for WordPress is vulnerable to Cross-Site Request Forgery (CSRF) in all versions up to and including 1.0. This is due to a completely broken nonce validation in the enter_mpcpl_login_options() function, which contains an inverted check (if wp_verify_nonce(...) { return false; }) and is missing the required action parameter for wp_verify_nonce(). As a result, the nonce check is effectively dead code: it never blocks malicious requests because a CSRF-supplied empty/invalid nonce always returns false, satisfying the inverted condition to continue execution. Furthermore, the settings-update handler is hooked on init without any capability check. This makes it possible for unauthenticated attackers to modify all plugin setting, including login page background, logo URL, image dimensions, button colors, and login message, by tricking a logged-in administrator into submitting a crafted request.	2026-06-24	4.3	CVE-2026-6292
masteriyo--Masteriyo LMS Course Builder, Quizzes & Certificates	The Masteriyo LMS - LMS Course Builder, Quizzes & Certificates plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 2.2.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with student-level access and above, to modify the description (post content) of arbitrary course announcements authored by instructors or administrators.	2026-06-27	4.3	CVE-2026-11773
mastodon--mastodon	Mastodon is a free, open-source social network server based on ActivityPub. Prior to 4.5.10, 4.4.17, and 4.3.23, Mastodon's normalization of incoming activities signed with Linked-Data Signatures does not sufficiently protect the activities from a certain class of spoofing, allowing	2026-06-24	6.5	CVE-2026-48028

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	threat actors to remove JSON entries from valid signed activities from a third-party actor. This vulnerability is fixed in 4.5.10, 4.4.17, and 4.3.23.			
mastodon--mastodon	Mastodon is a free, open-source social network server based on ActivityPub. Prior to 4.5.10, 4.4.17, and 4.3.23, Mastodon's normalization of incoming activities signed with Linked-Data Signatures does not sufficiently protect the activities from a certain class of spoofing, allowing attackers to re-arrange a valid signed JSON-LD activity from a third-party actor to have it processed differently. This vulnerability is fixed in 4.5.10, 4.4.17, and 4.3.23.	2026-06-24	5.3	CVE-2026-46349
mastodon--mastodon	Mastodon is a free, open-source social network server based on ActivityPub. From 4.3.0 until 4.5.11 and 4.4.18, Mastodon has a feature to let websites credit authors of their articles. To prevent false attribution claims, Mastodon uses the attributionDomains JSON-LD term, however, an error in how it is defined makes Linked Data Signatures on the toot:attributionDomains property ineffective. An attacker can arbitrarily modify the attributionDomains value of a legitimately signed Update activity and bypass Mastodon's signature verification. This vulnerability is fixed in 4.5.11 and 4.4.18.	2026-06-24	5.3	CVE-2026-50128
Mattermost--github.com/mattermost/mattermost/server/public	The Mattermost Go module github.com/mattermost/mattermost/server/public versions < v0.1.22 fail to validate path parameters when constructing API route paths which allows an attacker to redirect API calls to unintended endpoints via crafted IDs containing path traversal components. Mattermost Advisory ID: MMSA-2025-00532	2026-06-26	5.4	CVE-2026-13426
Mattermost--Mattermost	Mattermost versions 10.11.x <= 10.11.18, 11.6.x <= 11.6.3, 11.5.x <= 11.5.6 fail to validate attachment URLs against internal or private IP ranges in the Mattermost Agents plugin MCP server which allows an attacker with access to the MCP server in stdio mode to perform server-side request forgery (SSRF) and exfiltrate data from internal network services via supplying internal URLs as file attachments in post creation requests.. Mattermost Advisory ID: MMSA-2026-00635	2026-06-26	6.5	CVE-2026-4339
Mattermost--Mattermost	Mattermost versions 11.7.x <= 11.7.0, 11.6.x <= 11.6.2, 11.5.x <= 11.5.5, 10.11.x <= 10.11.17 Fail to validate channel ownership of an existing subscription before applying edits which allows an authenticated attacker to hijack subscriptions from channels they have no access to via a crafted PUT request to the subscription edit endpoint.. Mattermost Advisory ID: MMSA-2026-00650	2026-06-22	6.4	CVE-2026-6062
Mattermost--Mattermost	Mattermost versions 11.7.x <= 11.7.0, 11.6.x <= 11.6.2, 11.5.x <= 11.5.5, 10.11.x <= 10.11.17 fail to authenticate Atlassian Connect installed callbacks, allowing a remote unauthenticated attacker to inject a rogue sharedSecret and disrupt the Jira integration via POST to /ac/installed during the pending-install window.. Mattermost Advisory ID: MMSA-2026-00654	2026-06-22	6.4	CVE-2026-6673
Mattermost--Mattermost	Mattermost Plugins versions <=11.6 10.18.11 11.3.6 11.6.5.0 fail to sanitize error responses from the OpenAI API before logging, which allows a user with access to server logs or support packets to obtain a valid or partially reconstructable OpenAI API key via inspection of mattermost.log entries	2026-06-26	6.8	CVE-2026-9699

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	generated during authentication failures. Mattermost Advisory ID: MMSA-2026-00609			
Mattermost--Mattermost	Mattermost versions 11.7.x <= 11.7.0, 11.6.x <= 11.6.2, 11.5.x <= 11.5.5, 10.11.x <= 10.11.17 fail to enforce administrator authorization on the {{setDefaultInstance}} call within the {{/gitlab connect}} command handler, which allows any authenticated user to overwrite the global default GitLab instance configuration via the {{/gitlab connect <instance-name>}} slash command.. Mattermost Advisory ID: MMSA-2026-00644	2026-06-22	5.4	CVE-2026-5139
Mattermost--Mattermost	Mattermost versions 11.7.x <= 11.7.0, 11.6.x <= 11.6.2, 11.5.x <= 11.5.5, 10.11.x <= 10.11.17 fail to invalidate cached authentication state for active WebSocket connections during global session revocation, which allows a user with an existing WebSocket connection to remain authenticated and continue receiving real-time events until the cached session expires or the client reconnects.. Mattermost Advisory ID: MMSA-2026-00664	2026-06-22	4.3	CVE-2026-9162
Mattermost--Mattermost Google Drive Plugin	The Mattermost Google Drive plugin before version 1.1.0 fails to validate channel membership in the file creation endpoint, allowing authenticated users with a connected Google account to share Google Drive files to unauthorized private channels and disclose private channel membership.	2026-06-25	4.2	CVE-2026-2299
maxfoundry--MaxButtons Create buttons	The MaxButtons - Create buttons plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'view' parameter in all versions up to, and including, 9.8.5 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	2026-06-27	6.1	CVE-2026-13245
Mervin Praisson--Featured Image	Author Cross Site Scripting (XSS) in Featured Image <= 2.1 versions.	2026-06-26	6.5	CVE-2026-57431
metagauss--ProfileGrid User Profiles, Groups and Communities	The ProfileGrid - User Profiles, Groups and Communities plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'pm_author_message' parameter in the pm_send_message_to_author function in all versions up to, and including, 5.9.9.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The vulnerability was partially patched in version 5.9.8.5.	2026-06-23	6.4	CVE-2026-4610
metagauss--RegistrationMagic Custom Registration Forms, User Registration, Payment, and User Login	The RegistrationMagic - Custom Registration Forms, User Registration, Payment, and User Login plugin for WordPress is vulnerable to Authentication Bypass via Insufficient Verification of Data Authenticity in all versions up to and including 6.0.8.6. This is due to the PayPal IPN `callback` handler being registered as a nopriv AJAX action with no authentication or nonce requirement, and critically because the handler updates the payment log database row with attacker-controlled POST data - including `payment_status` and the `custom` field encoding the target `user_id` - before PayPal IPN validation is performed, meaning the database remains poisoned even when validation subsequently fails. This makes it possible for unauthenticated attackers to authenticate as any WordPress user, including administrators, by submitting a forged IPN request that overwrites a payment log entry's `user_id` with that of a target account, then visiting the success return URL with a legitimately	2026-06-27	5.3	CVE-2026-9242

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	obtained security hash to cause the plugin to issue real WordPress authentication cookies for the targeted account.			
Mintplex-Labs--anything-llm	AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. Prior to 1.13.0, on Windows, the document folder listing route can accept an encoded absolute Windows path that resolves outside the intended documents directory. The shared path containment helper rejects POSIX-style "../" traversal but does not reject Windows-style parent paths returned by path.relative(), such as "..". This vulnerability is fixed in 1.13.0.	2026-06-24	4.3	CVE-2026-48789
mirsoftware--MIR blocks and shortcodes	The MIR blocks and shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title' attribute (and other attributes such as 'ready_animation_text') of the 'msc_stats' shortcode in versions up to, and including, 1.0.0. This is due to insufficient input sanitization and output escaping on user supplied shortcode attributes inside the msc_stats() rendering function. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-24	6.4	CVE-2026-8896
MLflow--MLflow	A vulnerability has been found in MLflow up to 4666cffc7912ea606d592fc38d6a75e2935f65e7. The impacted element is an unknown function of the component Experiment-scoped Label Schema CRUD API. Such manipulation leads to missing authorization. It is possible to launch the attack remotely. A high complexity level is associated with this attack. The exploitability is regarded as difficult. The exploit has been disclosed to the public and may be used. A reply to the GitHub issue explains, that "[t]he labeling schema PR has not been merged yet. The auth handlers will be added before the release."	2026-06-28	5	CVE-2026-13484
motioneye-project--motioneye	motionEye (mEye) is an online interface for motion software, which is a video surveillance program with motion detection. Versions prior to 0.44.0 are vulnerable to path traversal in the picture and movie API endpoints, such as /picture/{id}/preview/{filename}. Neither the API handlers, nor the mediafiles.py functions such as get_media_preview() check for .. sequences in the filename parameter, except for get_media_content(). This allows an authenticated user with normal (non-admin) privileges to read arbitrary files from the filesystem as the motionEye process user, such as: /etc/passwd, /etc/shadow, motionEye config files containing password hashes and plaintext passwords, SSH keys, and other cameras' surveillance footage. This issue has been fixed in version 0.44.0.	2026-06-24	6.5	CVE-2026-31978
motioneye-project--motioneye	motionEye (mEye) is an online interface for motion software, a video surveillance program with motion detection. Versions prior to 0.44.0 create the configuration file /etc/motioneye/motion.conf with 644 permissions (-rw-r--r--), making it readable by any local user on the system. This file contains sensitive data including the admin password hash, which can be leveraged by other vulnerabilities to escalate privileges. Additionally, per-camera configuration files (camera-*.conf) are also created with the same 644 permissions, potentially exposing camera-specific credentials and settings. The exposed SHA1 admin password hash can be cracked offline to recover the plaintext password, used directly to forge authenticated admin API requests via the signature authentication weakness (GHSA-45h7-499j-7ww3), and chained with the OS command	2026-06-24	5.5	CVE-2026-32315

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	injection flaw (CVE-2025-60787) to escalate a local unprivileged user to the Motion daemon user (often root), enabling full system compromise. This issue has been fixed in version 0.44.0.			
motordesk--MotorDesk	The MotorDesk plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1.2. This is due to missing or incorrect nonce validation on the motordesk_admin_home function. This makes it possible for unauthenticated attackers to update the plugin's configuration settings, including the search page URI and custom template directory path via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-24	4.3	CVE-2026-9724
myCred--License Manager for WooCommerce	Unauthenticated Insecure Direct Object References (IDOR) in License Manager for WooCommerce <= 3.0.15 versions.	2026-06-25	6.5	CVE-2026-56013
MyScale--MyScaleDB	A security flaw has been discovered in MyScale MyScaleDB up to 1.8.0. This vulnerability affects the function SegmentId::getCacheKey in the library src/VectorIndex/Common/SegmentId.h. The manipulation results in insufficient verification of data authenticity. It is possible to launch the attack remotely. A high complexity level is associated with this attack. It is stated that the exploitability is difficult. The exploit has been released to the public and may be used for attacks. The pull request to fix this issue awaits acceptance.	2026-06-28	5	CVE-2026-13513
n8n--n8n	n8n before 1.123.25 (1.x) and before 2.11.2 (2.x), with the fix also included in 2.12.0, contains a stored cross-site scripting vulnerability in the Form Trigger node's CSS sanitization that allows authenticated users to inject malicious scripts. Attackers with workflow creation permissions can inject XSS payloads that execute persistently for all form visitors, enabling form hijacking and phishing attacks.	2026-06-24	5.4	CVE-2026-56358
n8n--n8n	n8n before 1.123.15 and 2.5.0 contains a webhook forgery vulnerability in the GitHub Webhook Trigger node that fails to implement HMAC-SHA256 signature verification. Attackers who know the webhook URL can send unsigned POST requests to trigger workflows with arbitrary data, spoofing GitHub webhook events.	2026-06-22	4	CVE-2026-56357
nanocoai--nanoclaw	NanoClaw before 2.1.17 contains a privilege escalation vulnerability in the handleApprovalsResponse function that fails to verify responder role authorization. Attackers with a valid questionId can approve or reject privileged actions like package installation by submitting approval response payloads without proper role validation.	2026-06-23	6.5	CVE-2026-56402
nanocoai--nanoclaw	NanoClaw before 2.1.17 contains a symlink following vulnerability in forwardAttachedFiles that allows container-controlled agents to exfiltrate host-readable files. The host validates attachment filenames using only isSafeAttachmentName before copying with fs.copyFileSync, which follows symlinks without containment checks, allowing malicious agents to disclose arbitrary host files.	2026-06-23	5.5	CVE-2026-56692
nanocoai--nanoclaw	NanoClaw before 2.1.17 contains a privilege escalation vulnerability in the create_agent delivery-action handler that performs privileged central-database writes without host-side authorization checks. Confined agent containers can invoke create_agent to create arbitrary agent groups,	2026-06-23	5.5	CVE-2026-56693

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	container configurations, and destinations, escalating beyond their intended confinement boundary.			
nanocoai--nanoclaw	NanoClaw before 2.1.0 contains a privilege escalation vulnerability in the channel-registration approval flow where handleChannelApprovalResponse fails to validate admin privileges over target agent groups. Scoped admins can submit forged or stale connect callback values to wire messaging channels into out-of-scope agent groups, exposing unauthorized groups to unapproved channels and enabling unauthorized observation or control of restricted agent group activity.	2026-06-23	5.4	CVE-2026-56694
Nelio Software--Nelio Content	Contributor Broken Access Control in Nelio Content <= 4.3.4 versions.	2026-06-26	4.3	CVE-2026-57648
NetworkConfiguration--dhcpcd	dhcpcd through 10.3.2, fixed in commit 708b4a5, contains a memory leak vulnerability in the IPv6 Router Advertisement route information handling that allows an unauthenticated same-link attacker to cause denial of service by sending crafted Router Advertisements. Attackers can repeatedly send Router Advertisements containing Route Information options with a lifetime of zero, triggering unfreed allocations in routeinfo_findalloc() that cause linear memory exhaustion and eventual daemon crash.	2026-06-23	6.5	CVE-2026-56116
NetworkConfiguration--dhcpcd	dhcpcd through 10.3.2, fixed in commit 5733d3c, contains a heap use-after-free vulnerability that allows unauthenticated same-link attackers to crash the daemon by sending a crafted DHCPv6 RENEW reply with RFC6603 OPTION_PD_EXCLUDE and both preferred and valid lifetimes set to zero. Attackers acting as or impersonating a DHCPv6 server can trigger dhcp6_deprecatedele() to free a delegated child address while an outer TAILQ_FOREACH_SAFE iterator in dhcp6_deprecateaddrs() still holds the freed pointer, causing a use-after-free when TAILQ_REMOVE is reached.	2026-06-23	5.3	CVE-2026-56113
NetworkConfiguration--dhcpcd	dhcpcd through 10.3.2, fixed in commit 2f00c7b, contains a one-byte stack out-of-bounds write vulnerability in dhcp6_makemessage() in src/dhcp6.c that allows unauthenticated same-link attackers to write beyond a fixed local buffer by serializing an oversized RFC6603 OPTION_PD_EXCLUDE option body. Attackers can send a crafted DHCPv6 ADVERTISE message containing an IA_PD IAPREFIX /0 with a valid OPTION_PD_EXCLUDE using an exclude prefix length of /121 through /128 to trigger the out-of-bounds write and potentially corrupt adjacent stack memory.	2026-06-23	5.3	CVE-2026-56114
NetworkConfiguration--dhcpcd	dhcpcd through 10.3.2, fixed in commit 78ea09e, contains a heap use-after-free vulnerability in the control socket handling within src/control.c that allows local unprivileged attackers to trigger memory corruption when privilege separation is disabled. Attackers can connect to the control socket and send a privileged command such as -x, causing control_recvdata() to free the client object while the same READ+HANGUP event subsequently reaches control_hangup() with the stale pointer, resulting in a use-after-free condition exploitable in deployments using --disable-privsep or where privsep initialization has failed with the control socket operating in mode 0666.	2026-06-23	4.7	CVE-2026-56117
Nexcess--WPComplete	Subscriber Broken Access Control in WPComplete <= 2.9.5.5 versions.	2026-06-26	5.4	CVE-2026-57661

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nghttp2--nghttp2	nghttp2's nghttpx proxy through 1.69.0 forwards an HTTP/1.1 Upgrade request that also carries a Content-Length header and body onto reusable keep-alive backend connections, re-adding the Upgrade and Connection headers while passing Content-Length verbatim. A backend that resolves the resulting ambiguous message in the attacker's favor enables HTTP request/response smuggling and cross-client response-queue poisoning.	2026-06-28	5.4	CVE-2026-58055
nicolargo--glances	Glances is an open-source system cross-platform monitoring tool. Prior to 4.5.5, the Glances XML-RPC server (glances -s, implemented in glances/server.py) does not validate the HTTP Host header, leaving it vulnerable to DNS rebinding attacks. An attacker can exploit DNS rebinding to exfiltrate the full system monitoring dataset from a victim's browser. This vulnerability is fixed in 4.5.5.	2026-06-25	5.3	CVE-2026-46611
nK--Ghost Kit	Contributor Cross Site Scripting (XSS) in Ghost Kit <= 3.6.0 versions.	2026-06-26	6.5	CVE-2026-57651
Nmap--Nmap	Nmap through 7.99 does not keep the IPv6 extension-header walk within the captured packet in ipv6_get_data_primitive (libnetutil/netutil.cc), so the pointer advances past the buffer and the remaining-length computation underflows to a large value. A scanned target or on-path attacker returning a crafted IPv6 response with a truncated extension header can trigger out-of-bounds reads and a crash during raw IPv6 scans.	2026-06-28	6.5	CVE-2026-58058
nocodb--nocodb	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, a reflected XSS vulnerability exists in the Page Leaving Warning page. The ncRedirectUrl and ncBackUrl query parameters are used in window.location.href and <a> tag bindings without validation, allowing javascript: URI injection. This vulnerability is fixed in 2026.04.1.	2026-06-23	6.1	CVE-2026-46547
nocodb--nocodb	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.4, the uploadViaURL path in the v1/v2 attachment API did not enforce NC_ATTACHMENT_FIELD_SIZE against the remote content-length or against the response stream. An authenticated user (Editor+) could direct the server to download arbitrarily large files, exhausting disk space and causing denial of service. In packages/nocodb/src/services/attachments.service.ts, the HEAD probe read content-length but never compared it to NC_ATTACHMENT_FIELD_SIZE; the subsequent storageAdapter.fileCreateByUrl() performed the download without maxContentLength. This vulnerability is fixed in 2026.04.4.	2026-06-23	6.5	CVE-2026-46551
nocodb--nocodb	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, an authenticated user with columnAdd permission on a Postgres-backed base can inject arbitrary SQL into the formula engine via the optional direction argument of ARRAYSORT(...). The value is unrestricted by formula validation and embedded into a knex.raw ORDER BY clause, executing during column creation and on every subsequent record read of the formula column. The vulnerability is specific to the Postgres mapping for ARRAYSORT in packages/nocodb/src/db/functionMappings/pg.ts. This vulnerability is fixed in 2026.04.1.	2026-06-23	6	CVE-2026-47375
nocodb--nocodb	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, the refresh-token cookie was set with httpOnly: true but missing both the secure flag and the sameSite attribute. Over plain HTTP	2026-06-23	5.4	CVE-2026-46550

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the cookie could be intercepted on the network; without sameSite, browsers attached it to cross-site POSTs, enabling CSRF against the token-refresh endpoint. This vulnerability is fixed in 2026.04.1.			
nocodb--nocodb	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, shared-base sessions were granted the same base-member capabilities as authenticated viewers. Using only the shared-base UUID (xc-shared-base-id), an attacker could enumerate base members and invite an arbitrary email into the base as a real member. The invited user could then redeem the invite via the normal signup flow and retain authenticated access even after the owner revoked the shared link. Shared-base sessions were mapped to ProjectRoles.VIEWER in packages/nocodb/src/strategies/base-view.strategy/base-view.strategy.ts, and packages/nocodb/src/utlis/acl.ts granted baseUserList and userInvite to that role. The shared frontend (packages/nc-gui/composables/useApi/interceptors.ts) deliberately removed auth headers in favour of the shared-base header, but the ACL middleware did not distinguish shared sessions from genuine viewers. This vulnerability is fixed in 2026.04.1.	2026-06-23	5.8	CVE-2026-46552
nocodb--nocodb	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, the request-filtering-agent SSRF protection was non-functional in the four notification webhook plugins (Slack, Discord, Mattermost, Teams) because httpAgent / httpsAgent were passed as part of the request body rather than the axios config. An authenticated user with hook-creation permission could direct outbound POST requests to arbitrary internal hosts. This vulnerability is fixed in 2026.04.1.	2026-06-23	4.3	CVE-2026-46548
nodeca--js-yaml	js-yaml is a JavaScript YAML parser and dumper. Prior to 4.2.0, a crafted YAML document can trigger algorithmic CPU exhaustion in js-yaml merge-key processing (<<) by repeating the same alias many times in a merge sequence. This causes quadratic parse-time behavior relative to input size and can block a Node.js worker/event loop for seconds with a relatively small payload (tens of KB), resulting in denial of service. The issue is in merge handling inside lib/loader.js. This vulnerability is fixed in 4.2.0.	2026-06-22	5.3	CVE-2026-53550
Noor Alam--Gmail SMTP	Unauthenticated Cross Site Request Forgery (CSRF) in Gmail SMTP <= 1.2.3.19 versions.	2026-06-26	4.3	CVE-2026-57657
notepad-plus-plus--notepad-plus-plus	Notepad++ is a free and open-source source code editor. Prior to 8.9.6.1, a local process in the same interactive Windows session can send a malformed WM_COPYDATA message to Notepad++ using the COPYDATA_FULL_CMDLINE path. The handler appears to process COPYDATASTRUCT.lpData as an unbounded NUL-terminated wchar_t* instead of enforcing COPYDATASTRUCT.cbData. This vulnerability is fixed in 8.9.6.1.	2026-06-26	5	CVE-2026-48770
nrwl--nx	Nx is a monorepo solution for TypeScript and polyglot codebases. From 17.0.4 until 22.7.2 and 23.0.0-beta.2, the local HTTP server started by nx graph sent Access-Control-Allow-Origin: * on every response, letting any website a developer visited read the server's responses cross-origin - including the full project graph and the output of the /help endpoint, which runs a target's configured help command. The practical impact is typically cross-origin information disclosure, but can be arbitrary command	2026-06-26	5.9	CVE-2026-54753

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	injection in rare cases. This vulnerability is fixed in 22.7.2 and 23.0.0-beta.2.			
Nuxt--Nuxt	Nuxt versions 4.0.0 before 4.4.7 and 3.x before 3.21.7 contain a server-side open redirect vulnerability in navigateTo that fails to properly validate path-normalized payloads like ../../evil.com and ../../evil.com. Attackers can bypass external-host checks using path-normalization techniques to redirect users to attacker-controlled sites via the Location header or meta-refresh, enabling phishing and OAuth authorization-code theft.	2026-06-22	6.1	CVE-2026-56326
Nuxt--Nuxt	Nuxt versions 4.0.0 before 4.4.7 and 3.x before 3.21.7 accept protocol-relative paths such as //evil.com in the reloadNuxtApp function; these pass the script-protocol check but resolve to a cross-origin URL against the current page protocol. Attackers can inject paths like //evil.com to redirect users to attacker-controlled hosts, enabling phishing and OAuth authorization-code theft.	2026-06-22	6.1	CVE-2026-56697
Nuxt--Nuxt	Nuxt versions 4.0.0 before 4.4.7 and 3.x before 3.21.7 fail to validate script-capable URLs in the navigateTo open option, allowing client-side script execution. Attackers can supply javascript: URLs through the open parameter to execute arbitrary scripts in the application's origin when user-controlled input is passed to navigateTo.	2026-06-22	6.1	CVE-2026-56698
Nuxt--Nuxt	Nuxt 4.0.0 before 4.4.7 and 3.18.0 before 3.21.7, when running the development server (nuxt dev) on Linux, binds the vite-node IPC server to an abstract-namespace Unix socket without permission restrictions, allowing local users to enumerate and connect. Unprivileged co-resident users can exploit the unprotected module request handler to read arbitrary files such as .env and SSH keys through the SSR plugin pipeline. Production builds are unaffected, as the IPC server runs only in development.	2026-06-23	5.5	CVE-2026-56301
Omnisend--Email Marketing for WooCommerce by Omnisend	Subscriber Broken Access Control in Email Marketing for WooCommerce by Omnisend <= 1.19.0 versions.	2026-06-26	5.4	CVE-2026-57632
Opal_WP--Auros Core	Unauthenticated Content Injection in Auros Core <= 5.3.1 versions.	2026-06-26	5.3	CVE-2025-64637
open-telemetry--opentelemetry-js	opentelemetry-js is the OpenTelemetry JavaScript Client. Prior to 2.8.0, W3CBaggagePropagator.extract() in @opentelemetry/core does not enforce size limits when parsing inbound baggage HTTP headers. The W3C Baggage specification recommends a maximum of 8,192 bytes and 180 entries; these limits were only enforced on the outbound (inject()) path, not on the inbound (extract()) path. Parsing oversized baggage causes memory allocation proportional to the header size without any cap. This vulnerability is fixed in 2.8.0.	2026-06-22	5.3	CVE-2026-54285
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, POST /api/chat/completions accepts an image_url.url value that, when it does NOT start with http://, https://, or data:image/, is interpreted as a file id and resolved against the global file table with no ownership check. an authenticated user can therefore set image_url.url to another user's file id, the server reads that file from disk, base64-encodes it, and injects the data URI into the LLM request. the	2026-06-23	6.5	CVE-2026-54009

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	user then prompts the LLM to describe / OCR the file and reads the content back. This vulnerability is fixed in 0.9.6.			
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, Open WebUI's prompt version-history endpoints authorize the prompt_id in the URL but then act on caller-supplied history IDs without verifying that the history row belongs to that prompt (history_entry.prompt_id == prompt.id). This affects /api/v1/prompts/id/{prompt_id}/history/diff, /api/v1/prompts/id/{prompt_id}/update/version, and /api/v1/prompts/id/{prompt_id}/history/{history_id}. An authenticated user with access to any prompt they control, plus a victim prompt_history.id, can read or delete another user's private prompt history. This vulnerability is fixed in 0.9.6.	2026-06-23	6.4	CVE-2026-54015
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, Open WebUI added collection-level ACL checks, but the patch can still be bypassed when Milvus multitenancy mode is enabled. The ACL allows unknown non-KB collection names as legacy/ephemeral collections. In Milvus multitenancy mode, that user-controlled collection name becomes a resource_id and is interpolated into a Milvus expression without escaping. This is caused by an incomplete fix for CVE-2026-44560 This vulnerability is fixed in 0.9.6.	2026-06-23	6.5	CVE-2026-54019
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, several direct, index-addressed Ollama proxy routes accept a caller-supplied url_idx path parameter and use it as a raw index into the admin-configured OLLAMA_BASE_URLS list. Access control on these routes validates only whether the user may use the requested model, never which backend the request is routed to. Any authenticated user can append an arbitrary url_idx to force their request onto an Ollama backend they were never authorized to reach, including internal, higher-privilege, or explicitly admin-disabled backends. This vulnerability is fixed in 0.9.6.	2026-06-23	6.3	CVE-2026-54021
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.8.11, the ydoc:document:join Socket.IO handler checks note ownership only when the document_id starts with note: (colon). However, the YdocManager storage layer normalizes all document IDs by replacing colons with underscores (document_id.replace(":", "_")). An attacker can join a document room using note_<id> (underscore) instead of note:<id> (colon), bypassing the authorization check entirely while accessing the same underlying Yjs document. The server then returns the full document state, leaking the victim's private note contents. This vulnerability is fixed in 0.8.11.	2026-06-23	5.3	CVE-2026-54022
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, POST /api/v1/calendars/events/{event_id}/update validates that the caller has write access to the calendar the event currently belongs to, but does not validate the destination calendar_id supplied in the request body. The model layer then persists the new calendar_id unconditionally. A regular user-role account can therefore create an event in their own calendar and immediately move it into any other user's calendar whose ID they know -	2026-06-23	4.3	CVE-2026-54006

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bypassing the authorization check that create_event correctly performs. This vulnerability is fixed in 0.9.6.			
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, a path traversal vulnerability exists in open-webui's cache file serving endpoint that allows any authenticated user to read files from sibling directories outside the intended cache directory, by exploiting an incomplete startswith containment check that lacks a trailing path separator. The root cause is that serve_cache_file() in open_webui/main.py validates the resolved path with file_path.startswith(os.path.abspath(CACHE_DIR)) - without appending os.sep. This allows any path resolving to a sibling directory whose name begins with cache (e.g. cache_sibling, cache_backup, cached_models) to pass validation. This vulnerability is fixed in 0.9.6.	2026-06-23	4.3	CVE-2026-54014
open-webui--open-webui	Open WebUI is a self-hosted artificial intelligence platform designed to operate entirely offline. Prior to 0.9.6, Open WebUI has a Broken Object Level Authorization (BOLA) vulnerability in the builtin search_knowledge_files tool. When native function calling is enabled and the selected model has no attached knowledge bases, an authenticated user can call search_knowledge_files with an arbitrary knowledge_id. The function then returns file metadata from that knowledge base without checking whether the user has read access. This allows unauthorized enumeration of private or restricted knowledge base files. This vulnerability is fixed in 0.9.6.	2026-06-23	4.3	CVE-2026-54016
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.3.2 and 17.4.0, a Missing Authorization vulnerability exists in OpenProject's CostReportsController. The rename and update actions allow any authenticated user to modify the name, filters, and grouping of any Public cost report in the system without verifying ownership or permission level. An attacker who discovers or guesses a public report's numeric ID can rename or overwrite its filter configuration without any warning to the report's owner. This vulnerability is fixed in 17.3.2 and 17.4.0.	2026-06-26	6.5	CVE-2026-44734
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.3.2 and 17.4.0, the GET /api/v3/shares endpoint returns share details for ALL work packages in a project to any user with the view_shared_work_packages permission. The authorization check operates at the project level only - it does not verify the requesting user can actually view each individual shared work package. This allows a regular project member to discover work package IDs and subjects (including confidential titles), which users have been granted shared access, what role level was assigned (Editor, Commenter, Viewer). This vulnerability is fixed in 17.3.2 and 17.4.0.	2026-06-26	6.5	CVE-2026-44735
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.4.0, the GET /api/v3/relations endpoint allows any authenticated user to retrieve relations - and the subject (title) of work packages they have no permission to view - by supplying an arbitrary work package ID in the involved, fromId, or told filter. This bypasses the Relation.visible scope due to a flawed performance optimization in RelationQuery. This vulnerability is fixed in 17.4.0.	2026-06-26	6.5	CVE-2026-44736

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.3.3 and 17.4.1, the HTML sanitizer grants <macro> elements unrestricted data-* attributes via :data wildcard. An attacker injects data-controller="poll-for-changes" into a work package description, causing Stimulus.js to mount a controller that fetches an attacker-uploaded attachment and passes it to renderStreamMessage(). This executes arbitrary Turbo Stream actions - including redirect_to - in every victim's authenticated browser session, redirecting them to an attacker-controlled server. This vulnerability is fixed in 17.3.3 and 17.4.1.	2026-06-26	6.4	CVE-2026-52781
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.4.0, OpenProject's rich text (markdown) rendering pipeline uses Sanitize::Config::RELAXED[:css] for inline style sanitization. This configuration permits essentially all CSS properties in style attributes on permitted HTML elements (figure, img, table, th, tr, td). This allows any authenticated user with write access to formattable text fields (work package descriptions, comments, project descriptions, news) to inject CSS. This vulnerability is fixed in 17.4.0.	2026-06-26	5.7	CVE-2026-44696
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.3.2 and 17.4.0, Business Logic Error on OpenProject through PATCH request to /api/v3/users/me permits to bypass password requirements. A password validation flaw in the change password behavior allows attackers to change a user's password only with an active session takeover. This vulnerability is fixed in 17.3.2 and 17.4.0.	2026-06-26	5.9	CVE-2026-44733
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.3.3 and 17.4.1, a cross-project IDOR / authorization context confusion in the Calendar and Team Planner modules allows a user with management permissions in one project to delete public Calendar or Team Planner Queries from another project where they do not have the corresponding management permissions. Both modules authorize the request against the project identified by :project_id in the URL, but the actual Query object is loaded later by :id from Query.visible(current_user) without verifying that the loaded Query belongs to the authorized project. As a result, an attacker can use permissions from Project A to delete shared/public Calendar or Team Planner views from Project B, causing integrity impact and limited availability impact for users relying on those shared views. This vulnerability is fixed in 17.3.3 and 17.4.1.	2026-06-26	5.4	CVE-2026-52779
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.3.2 and 17.4.0, the web application's meetings filter feature leaks whether a given user ID corresponds to a valid account and discloses the user's full name, allowing an attacker to enumerate all existing user accounts by probing user IDs and observing differences in the server response. This vulnerability is fixed in 17.3.2 and 17.4.0.	2026-06-26	4.3	CVE-2026-44731
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.3.2 and 17.4.0, OpenProject exposes a document update endpoint used to modify existing documents. The target document is loaded with visibility checks and then updated. During update, attacker-controlled attributes are applied to the persisted record before authorization is enforced. As a result, a user without :manage_documents in the source project can move and modify foreign project documents by	2026-06-26	4.3	CVE-2026-44732

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	setting project_id in a single PATCH request. This vulnerability is fixed in 17.3.2 and 17.4.0.			
opf--openproject	OpenProject is open-source, web-based project management software. Prior to 17.4.0, `GET /api/v3/meetings/:meeting_id/agenda_items/:agenda_item_id` discloses private work package data from a linked work package that belongs to a private/inaccessible project. This vulnerability is fixed in 17.4.0.	2026-06-26	4.3	CVE-2026-49355
osiris8--Osiris Signature Banner	The Osiris Signature Banner plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.5. This is due to missing or incorrect nonce validation on a function. This makes it possible for unauthenticated attackers to update settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-24	6.1	CVE-2026-8905
owencutajar--EntreDroppers	The EntreDroppers plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via PHP_SELF Parameter in all versions up to, and including, 1.1.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. The payload is delivered via attacker-controlled path-info in the URL (e.g., /wp-admin/admin.php/"><script>alert(0)</script>/?page=EntreDroppers.php), which PHP_SELF reflects directly into the form action attribute.	2026-06-24	6.1	CVE-2026-8628
paradigmatools--Avalon23 Products Filter for WooCommerce	The Avalon23 Products Filter for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'avalon23_qr' shortcode in all versions up to, and including, 1.1.6. This is due to insufficient input sanitization and output escaping on user-supplied shortcode attributes (notably 'title' and 'fixed_link') which are concatenated directly into single-quoted HTML attributes by the AVALON23_HELPER::draw_html_item() helper without esc_attr() or any other encoding. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-24	6.4	CVE-2026-8865
peregrinethemes--Hester Core	Author Cross Site Scripting (XSS) in Hester Core <= 1.1.8 versions.	2026-06-26	5.9	CVE-2026-57656
phpseclib--phpseclib	phpseclib is a PHP secure communications library. From 0.1.1 until 1.0.30, 2.0.55, and 3.0.54, when an application validates an untrusted X.509 certificate with phpseclib, X509::validateSignature() reads a URL out of that certificate's Authority Information Access (AIA) extension and connects to it. Attacker who supplies certificate fully controls host, port, and path of that connection. URL fetching is enabled by default, and no destination is blocked. An unauthenticated attacker can therefore make a validating server open connections to internal hosts and ports it should never reach, for example loopback 127.0.0.1, cloud metadata address 169.254.169.254, and internal-only services. This is a server-side request forgery (SSRF) caused by an insecure default. This vulnerability is fixed in 1.0.30, 2.0.55, and 3.0.54.	2026-06-22	5.8	CVE-2026-55599
pixelwelt--Image Sizes on Demand	The Image Sizes on Demand plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via PHP_SELF Server Variable in all versions up to, and including, 1.3 due to insufficient input sanitization and output	2026-06-24	6.1	CVE-2026-8622

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. The injected payload only executes in the context of an administrator, as the settings page requires the manage_options capability to render.			
pnpm--pnpm	pnpm is a package manager. Prior to 10.34.0 and 11.4.0, pnpm passes the lockfile-controlled git resolution.commit value to git fetch without a --separator or commit-format validation. For git dependencies fetched through the shallow-fetch path, a malicious lockfile can replace the expected 40-character commit hash with a Git option such as --upload-pack=<command>. For SSH and local transports, --upload-pack can execute the supplied command. HTTPS transports ignore --upload-pack, so the practical attack surface is primarily SSH or local git dependencies. This vulnerability is fixed in 10.34.0 and 11.4.0.	2026-06-25	6.4	CVE-2026-50014
pnpm--pnpm	pnpm is a package manager. Prior to 10.34.0 and 11.4.0, pnpm's tarball extraction worker skips integrity verification when the integrity field is absent from the lockfile resolution. If an attacker can both modify pnpm-lock.yaml to remove the integrity: field and cause the referenced registry URL to serve altered package content, pnpm install --frozen-lockfile can install the altered package without an integrity error. npm's npm ci enforces integrity by default; pnpm's behavior of silently skipping verification is a pnpm-specific fail-open gap. This vulnerability is fixed in 10.34.0 and 11.4.0.	2026-06-25	6.8	CVE-2026-50021
pnpm--pnpm	pnpm is a package manager. Prior to 10.34.0 and 11.4.0, `pnpm install` in non-frozen mode can accept new remote package content after detecting that the downloaded tarball does not match the integrity recorded in pnpm-lock.yaml. When a package is already locked with an integrity value, and the registry later serves different metadata and tarball content for the same package name and version, pnpm initially reports an integrity mismatch. However, plain pnpm install then performs a resolution repair, accepts the registry's new integrity, updates the lockfile, installs the new content, and exits successfully. This means the lockfile integrity check does not act as a hard stop by default. This vulnerability is fixed in 10.34.0 and 11.4.0.	2026-06-25	6.8	CVE-2026-50573
pnpm--pnpm	pnpm is a package manager. Prior to 10.34.2 and 11.5.3, pnpm and pacquet expanded \${ENV_VAR} placeholders from repository-controlled .npmrc and pnpm-workspace.yaml into registry request destinations and registry credentials. A malicious repository could cause dependency resolution to send victim environment secrets to an attacker-selected registry before lifecycle scripts run. This vulnerability is fixed in 10.34.2 and 11.5.3.	2026-06-25	6.5	CVE-2026-55180
pnpm--pnpm	pnpm is a package manager. Prior to 10.34.2 and 11.5.3, Manifest bin object keys such as "", ".", and ".." passed pnpm's bin-name guard. When a malicious package was installed globally, later global remove, update, or add-replacement flows could re-derive those names from the installed manifest and pass path.join(globalBinDir, binName) to removeBin. For "." this targets the global bin directory; for ".." this targets its parent. This vulnerability is fixed in 10.34.2 and 11.5.3.	2026-06-25	6.5	CVE-2026-55699

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
podman-container-tools--podman	Podman is a tool for managing OCI containers and pods. From 3.0.0 until 5.7.1, running a malicious container image where the WORKDIR path contains a symlink can create a directory or modify ownership on the host filesystem. Modified ownership is less likely to happen as that requires help from an untrusted/malicious process that mutates the host filesystem tree during dereferencing of the WORKDIR path, to trigger a race condition. This vulnerability is fixed in 5.7.1.	2026-06-26	5.3	CVE-2026-55686
poweradmin--poweradmin	Poweradmin is a web-based DNS administration tool for PowerDNS server. Versions prior to 4.2.4 and 4.3.3 are vulnerable to CSV Injection (Formula Injection) in its log export functionality. User-controlled data - specifically the username field - is written to exported CSV files without sanitizing formula trigger characters (=, +, -, @). When an administrator exports activity logs and opens the resulting CSV in a spreadsheet application (Microsoft Excel, LibreOffice Calc, Google Sheets), any formula stored in a username is executed by the application. This can be used for phishing attacks against administrators or data exfiltration. Versions 4.2.4 and 4.3.3 patch the issue.	2026-06-23	6.9	CVE-2026-47693
PowerDNS--Authoritative	An attacker can send a web request that causes unlimited memory allocation in the internal web server, leading to a denial of service. The internal web server is disabled by default.	2026-06-25	4.3	CVE-2026-42005
PowerDNS--DNSdist	An attacker might be able to cause outgoing TCP connections to backend to be stuck until a timeout occurs instead of being released immediately, by sending IXFR queries. This could be used to cause a denial of service if there is a limit to the number of concurrent connections to this backend, or if the process runs out of file descriptors.	2026-06-25	5.3	CVE-2026-40209
PowerDNS--DNSdist	An attacker can send crafted DNS over HTTP/3 queries, triggering an exception that prevents some buffer from being freed right away. The buffer will be freed at the end of the QUIC connection, but on some setups it might be possible to open enough concurrent DoH3 streams to trigger an out-of-memory condition, resulting in a denial of service.	2026-06-25	5.3	CVE-2026-40211
PowerDNS--DNSdist	An out-of-bounds read might happen when SetMacAddrAction is used, potentially resulting in uninitialized memory being sent over the network or a crash.	2026-06-25	4.8	CVE-2026-40210
PowerDNS--Recursor	ECS zero scoped answers are stored in the packet cache while they should not. This impacts only configurations that have ECS enabled;	2026-06-25	5.3	CVE-2026-40012
PowerDNS--Recursor	A malicious authoritative server can send a crafted zone via the ZoneToCache function that leads to a crash of the Recursor due to insufficient input validation.	2026-06-25	5.9	CVE-2026-42387
PowerDNS--Recursor	Incomplete validation of the SOA record present in a catalog zone might lead to a crash.	2026-06-25	5.9	CVE-2026-42388
PowerDNS--Recursor	This fix provides extra hardening for the 5.4.x branch by doing extra validation of incoming answers from authoritative servers.	2026-06-25	5.3	CVE-2026-42389
PowerDNS--Recursor	An invalid zone might pass ZONEMD validation while it should not. This is only relevant if ZoneToCache is configured with ZONEMD validation.	2026-06-25	5.3	CVE-2026-42390

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
PowerDNS--Recursor	Spoofing replies to Recursor might mark an IP of an authoritative server as not supporting EDNS, causing validation of DNSSEC records served by that server to fail.	2026-06-25	5.9	CVE-2026-52690
protobufjs--protobuf.js	protobufjs compiles protobuf definitions into JavaScript (JS) functions. Prior to 8.6.0 and 7.6.3, protobufjs accepted certain schema-derived names that could collide with properties used by protobufjs runtime helpers. The known affected names are fields named hasOwnProperty, field or oneof names such as \$type when loaded through protobufjs JSON/reflection descriptors, and service methods whose generated helper name is rpcCall. When affected message or service types were used, protobufjs could read schema-controlled data where it expected an own-property helper, reflected type metadata, or the base RPC helper. This could cause deterministic exceptions or recursive calls in affected decode post-checks, verification, object conversion, reflected JSON serialization, or protobufjs RPC helper invocation. This vulnerability is fixed in 8.6.0 and 7.6.3.	2026-06-22	5.3	CVE-2026-54269
protobufjs--protobuf.js	protobufjs compiles protobuf definitions into JavaScript (JS) functions. From 8.2.0 to 8.4.2, protobufjs preserved unknown wire elements in message.\$unknowns and did not provide a decode-time option to discard unknown fields before retaining them. A crafted protobuf payload containing many unknown fields could therefore cause a decoded message to retain substantially more memory than the input size would suggest, even when unknown-field round-tripping is not needed. protobufjs 8.5.0 added the relevant decode-time options, allowing applications that decode untrusted protobuf data to disable unknown-field retention during decode. protobufjs 8.6.2 flips the default so unknown fields are discarded unless explicitly opted into.	2026-06-22	5.3	CVE-2026-54270
Pylons--webob	WebOb provides objects for HTTP requests and responses. Prior to 1.8.10, the normalization of the HTTP Location header during a redirect is vulnerable to an open redirect: WebOb joins the redirect target to the request URI using Python's urljoin, and since Python 3.10 the underlying urlsplit strips ASCII tab, carriage return, and newline characters before parsing, so a redirect target containing such characters can be reinterpreted as a protocol-relative URL whose authority is an attacker-controlled host. This bypasses the CVE-2024-42353 fix that escaped a leading double slash, allowing an attacker who influences the redirect location to send users to an arbitrary external site instead of the intended one. This vulnerability is fixed in 1.8.10.	2026-06-22	6.1	CVE-2026-44889
RAGapp--RAGapp	A vulnerability has been found in RAGapp up to 0.1.5. Affected is the function FileHandler.upload_file/FileHandler.remove_file of the file src/ragapp/backend/controllers/files.py of the component Knowledge File Handler. Such manipulation leads to path traversal. The attack can be executed remotely. The exploit has been disclosed to the public and may be used. The pull request to fix this issue awaits acceptance.	2026-06-28	6.3	CVE-2026-13509
Rapid7--InsightConnect Finger Plugin	OS Command Injection vulnerability in Rapid7 InsightConnect Finger Plugin on Linux allows authenticated attackers to execute arbitrary OS commands via the user or host parameters due to insufficient input validation in shell command construction.	2026-06-25	6	CVE-2026-8664

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Rapid7--InsightConnect Markdown Plugin	Server-Side Cross-Site Scripting and Server-Side Request Forgery vulnerability in the markdown_to_pdf action of Rapid7 InsightConnect Markdown Plugin version 3.1.4 and earlier on Linux allows remote attackers to execute JavaScript server-side and make arbitrary outbound HTTP requests via crafted content embedded in Markdown input. The PDF rendering engine does not restrict script execution or outbound network access.	2026-06-26	4.8	CVE-2026-8661
Rapid7--InsightConnect RPM Plugin	OS Command Injection vulnerability in Rapid7 InsightConnect RPM Plugin on Linux allows authenticated attackers to execute arbitrary OS commands via the repo, key, or name parameters due to insufficient input sanitization in shell command construction.	2026-06-24	6	CVE-2026-8663
Rapid7--InsightConnect Sed Plugin	Arbitrary File Read vulnerability in Rapid7 InsightConnect Sed Plugin on Linux allows authenticated attackers to read arbitrary files via the expression parameter due to insufficient input validation.	2026-06-25	6.5	CVE-2026-9153
Rapid7--InsightConnect SQLmap Plugin	OS Command Injection vulnerability in Rapid7 InsightConnect SQLmap Plugin on Linux allows authenticated attackers to execute arbitrary OS commands via the api_host or api_port parameters during connection configuration due to insufficient input validation.	2026-06-25	6	CVE-2026-8659
Rapid7--InsightConnect Tcpdump Plugin	OS Command Injection vulnerability in Rapid7 InsightConnect Tcpdump Plugin on Linux allows authenticated attackers to execute arbitrary OS commands via the options or filter parameters due to insufficient input sanitization in shell command construction.	2026-06-25	6	CVE-2026-8658
Red Hat--Logging Subsystem for Red Hat OpenShift	A missing authorization flaw was found in the OpenShift Cluster Logging Operator. The operator creates and forwards ServiceAccount tokens to output destinations without verifying that the ClusterLogForwarder creator has permission to use those credentials, allowing a delegated editor to exfiltrate SA tokens and escalate privileges.	2026-06-23	6.8	CVE-2026-10609
Red Hat--Pen Drive Powered by Red Hat Lightspeed	A flaw was found in the Pen Drive report generator. Cluster-sourced data is rendered into HTML reports without proper escaping or sanitization. An attacker with cluster administrator privileges can inject a stored cross-site scripting (XSS) payload into cluster objects (such as ClusterVersion spec.channel) that executes in the browser of any user who opens the generated HTML report.	2026-06-25	6.9	CVE-2026-13083
Red Hat--Red Hat build of Apicurio Registry 3	A flaw was found in Apicurio Registry. The DocumentBuilderAccessor correctly blocks external DTD and schema access but does not disable DOCTYPE declarations or enable FEATURE_SECURE_PROCESSING. An attacker with artifact-write permission can upload XML documents with internal entity-expansion payloads (billion-laughs variant) that cause CPU and heap exhaustion, partially mitigated by the JAXP default 64,000 entity-expansion limit.	2026-06-25	6.5	CVE-2026-12993
Red Hat--Red Hat build of Keycloak 26.4	A flaw was found in Keycloak's client registration service. A remote attacker, possessing a previously issued Registration Access Token (RAT), could exploit this vulnerability to re-enable a client that an administrator had explicitly disabled. This bypasses security controls, allowing the attacker to reset the client's secret and potentially regain privileged API access. The primary impact includes unauthorized information disclosure and potential integrity compromise.	2026-06-25	6.5	CVE-2026-9705

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Red Hat--Red Hat build of Keycloak 26.4	A flaw was found in Keycloak. A realm administrator with the "manage-realm" role can exploit this vulnerability by submitting an arbitrary filesystem path as a keystore parameter when creating a key provider component. This allows the administrator to probe arbitrary filesystem paths, determining which files exist and are readable by the Keycloak process. This information disclosure could be used to identify high-value targets for follow-on attacks.	2026-06-25	4.9	CVE-2026-9083
Red Hat--Red Hat build of Keycloak 26.4	A flaw was found in org.keycloak.authorization. An authenticated user with a granted User-Managed Access (UMA) permission ticket for one resource can exploit this by using a specific permission request prefix to bypass per-resource access control. This allows the user to gain unauthorized access to all resources of that type within the same resource server, even if they do not have a ticket for those specific resources. This vulnerability requires the resource server to be configured in PERMISSIVE policy enforcement mode and affects typed resources with ownerManagedAccess enabled, where no explicit policy protects the resource type. The primary consequence is unauthorized information disclosure or modification of resources.	2026-06-25	4.6	CVE-2026-9799
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in the community.general Ansible collection's nexmo module. The module constructs HTTP requests to the Vonage/Nexmo SMS API by encoding API credentials (api_key and api_secret) into URL query parameters and sending them via GET requests. This causes credentials to be exposed in web server access logs, proxy logs, HTTP Referer headers, and network monitoring tools, despite the Ansible argument specification marking these parameters as no_log. An attacker with access to any of these logging or monitoring points can obtain the full API credentials and gain unauthorized access to the victim's Vonage/Nexmo account.	2026-06-23	6.5	CVE-2026-11820
Red Hat--Red Hat Enterprise Linux 10	Module: plugins/modules/keyring_info.py CVSS 3.1: 5.5 MEDIUM - AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N Issue: The module retrieves a passphrase from the OS native keyring (GNOME Keyring, macOS Keychain, Windows Credential Manager) and places it directly into result["passphrase"] with no output suppression, no no_log protection, and no documentation warning. Root Cause: Line 105 (protected): keyring_password=dict(type="str", required=True, no_log=True) Line 127 (NOT protected): result["passphrase"] = passphrase Observed Output: { "changed": false, "passphrase": "MyMasterP@sswOrd!SSH_Key_Secret" } Visible via register + debug: { "keyring_result": { "changed": false, "passphrase": "MyMasterP@sswOrd!SSH_Key_Secret" } } Impact: Master passwords, SSH key passphrases and service credentials appear in all Ansible output register: keyring_result followed by debug: var=keyring_result prints passphrase in full Ansible fact caching backends (Redis, JSON file, memcached) may persist the passphrase AWX/Tower job logs silently store the live credential Fix: module.exit_json(changed=False, passphrase=passphrase, _ansible_no_log=True) Also add a documentation warning requiring callers to use no_log: true at the task level. PoCs Fig 1: PoC execution showing passphrase in plaintext output Fig 2: Source code showing no_log=True on input (line 105) vs unprotected output (line 127)	2026-06-23	5.5	CVE-2026-11819
Red Hat--Red Hat Enterprise Linux 10	A heap-based buffer overflow was found in dnsmasq. When DNSSEC validation and query logging are both enabled, logging of DS or DNSKEY replies containing unsupported algorithm or digest types can cause dnsmasq to write past the end of an internal logging buffer. A remote	2026-06-22	5.9	CVE-2026-12725

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker able to supply such a DNS response may crash the dnsmasq process, resulting in denial of service.			
Red Hat--Red Hat Enterprise Linux 10	An out-of-bounds read vulnerability exists in dnsmasq's find_soa() function in src/rfc1035.c. When parsing NS section records, extract_name() is called with extrabytes=0, failing to validate that 10 additional bytes exist for fixed-length DNS record fields. A remote attacker controlling a DNS zone can exploit this via a crafted NXDOMAIN response to cause a 10-byte heap out-of-bounds read, potentially accessing stale data from prior transactions.	2026-06-23	5.3	CVE-2026-12969
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in OpenSSH. A local unprivileged attacker on a Linux client host can hijack client-side X11 forwarding connections. This is possible by pre-binding the preferred abstract X socket name when X11 forwarding is enabled and a local UNIX-domain X socket is used. A successful attack can compromise the confidentiality of forwarded X11 traffic, including sensitive window contents and input, and may allow some manipulation of the forwarded session.	2026-06-23	5	CVE-2026-55655
Red Hat--Red Hat Enterprise Linux 10	The fix for CVE-2026-2443 was regressed by a subsequent rework commit that replaced specific overflow checks with a general signed comparison. When a client sends a Range request with a suffix length exceeding the content size, the resulting negative start value is not properly clamped, leading to malformed HTTP 206 responses and log flooding.	2026-06-22	4.8	CVE-2026-12549
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in the GStreamer gst-plugins-bad package. When processing a malformed H.266/VVC video stream with a crafted aspect ratio indicator value, the H.266 parser performs an out-of-bounds read of up to 8 bytes from adjacent memory. This flaw allows an attacker to craft a malicious H.266 video file or stream that, when processed by a GStreamer-based application, could leak limited memory contents through video metadata, potentially exposing sensitive information from the application's address space.	2026-06-23	4.3	CVE-2026-12891
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in GStreamer's gst-plugins-bad package. When processing a specially crafted H.264 video file containing malformed MVC or SVC extension slice NAL units, a 1-byte heap out-of-bounds read can occur during parsing. This happens when the parser attempts to check slice boundary information without first verifying that the NAL unit contains enough data beyond the extension header. An attacker could exploit this by tricking a user into opening a malicious H.264 video file, potentially causing the application to crash or leak a single byte of heap memory.	2026-06-23	4.4	CVE-2026-12892
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in OpenSSH. A malicious SSH server can exploit a double free vulnerability in the Diffie-Hellman Group Exchange (DH-GEX) client path. This occurs during FIPS (Federal Information Processing Standards) mode known-group validation when the client processes attacker-controlled DH-GEX group parameters. Successful exploitation leads to client-side process termination, resulting in a Denial of Service (DoS).	2026-06-23	4.3	CVE-2026-55653
Red Hat--Red Hat OpenShift Virtualization 4	A flaw was found in KubeVirt's virt-handler domain notify server. The gRPC handlers for HandleDomainEvent and HandleK8SEvent derive the VMI identity (namespace/name) solely from the request body without validating it against the connection's origin. Each virt-launcher pod connects through a per-VMI pipe socket, but no identity tag is propagated	2026-06-24	6.5	CVE-2026-13208

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	from the pipe path to the server handlers. This allows a compromised virt-launcher process to send forged domain lifecycle events for any other VMI scheduled on the same node, causing virt-handler to erroneously update that VMI's state and disrupt its lifecycle management.			
Red Hat--Red Hat OpenShift Virtualization 4	A server-side request forgery (SSRF) flaw was found in KubeVirt's virt-api port-forward handler. When processing a port-forward request to a VirtualMachineInstance (VMI), virt-api reads the target IP from <code>vmi.Status.Interfaces[0].IP</code> and passes it directly to <code>net.Dial()</code> without validation. For VMIs using non-masquerade network bindings (bridge or secondary-only), this IP is reported by the QEMU guest agent running inside the VM and is fully controllable by the VM owner. An attacker with <code>kubevirt.io:edit</code> permissions can create a VM with a modified guest agent that reports an arbitrary IP address, then request port-forward to establish a bidirectional TCP tunnel from virt-api's cluster-internal network position to any routable destination, bypassing NetworkPolicy isolation.	2026-06-25	6.4	CVE-2026-13318
Red Hat--Red Hat OpenShift Virtualization 4	A flaw was found in KubeVirt's virt-handler network cache handling. The <code>WriteToCachedFile</code> function writes data to a launcher-rooted path using <code>os.WriteFile</code> and <code>os.Chown</code> without symlink protection. A user with access to the virt-launcher container can plant a symlink at the cache file path, causing virt-handler to follow it and overwrite an arbitrary host file with JSON content and change its ownership.	2026-06-25	4.2	CVE-2026-13218
Red Hat--Red Hat OpenShift Virtualization 4	A flaw was found in KubeVirt's network annotation generator. When a tenant creates a VirtualMachineInstance with a Multus network configuration, the supplied <code>networkName</code> value is written verbatim into the launcher pod's <code>v1.multus-cni.io/default-network</code> annotation without format validation or sanitization. The only admission check rejects empty strings; no DNS-1123 format validation, JSON detection, or special character rejection is performed. When the <code>ExternalNetResourceInjection</code> Beta feature gate is enabled (off by default, cluster-admin only), the NAD lookup that would otherwise catch malformed names is skipped by design. A tenant with <code>kubevirt.io:edit</code> permissions can inject a JSON-formatted <code>NetworkSelectionElement</code> array specifying an arbitrary namespace, NAD name, static IP address, and MAC address. Multus on the node parses this JSON and attaches the launcher pod to the specified network attachment in any namespace, enabling cross-namespace network access and IP/MAC impersonation on network segments normally segregated from tenant workloads. The <code>ExternalNetResourceInjection</code> feature gate was introduced in KubeVirt v1.8.0 (first shipped in OpenShift Virtualization 4.21).	2026-06-26	4.9	CVE-2026-13434
Red Hat--Red Hat Satellite 6.19	A flaw was found in <code>foreman-mcp-server</code> . This component utilizes two distinct logging mechanisms that can expose sensitive session and authentication data. One mechanism logs session identifiers, which are treated as authentication credentials, at an informational level. The other, when debug logging is enabled, incompletely sanitizes HTTP request headers, leading to the cleartext logging of sensitive information such as authorization tokens and API keys. This vulnerability can result in a confidentiality breach, as sensitive authentication data is persisted in plain text within container logs, increasing the risk if logs are forwarded to a centralized platform.	2026-06-23	6.2	CVE-2026-9073

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
reepaydenmark--Frisbii Pay	The Frisbii Pay plugin for WordPress is vulnerable to unauthorized modification of data due to missing capability checks on the 'upload_csv' and 'process_batch' functions in all versions up to, and including, 1.8.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to upload arbitrary CSV data and overwrite WooCommerce payment tokens, postmeta, and order meta records.	2026-06-27	6.5	CVE-2026-3462
rentmy--RentMy Real-Time Rental Management Plugin	The RentMy Real-Time Rental Management Plugin plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 4.0.4.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to read, create, update, and delete event records stored in the rentmy_events WordPress option, as well as overwrite the rentmy_locationId option.	2026-06-24	5.3	CVE-2026-8690
rhewlif--Donation Thermometer	Unauthenticated Broken Access Control in Donation Thermometer <= 2.2.7 versions.	2026-06-26	5.3	CVE-2025-64636
RocketChat--Rocket.Chat	Rocket.Chat is an open-source, secure, fully customizable communications platform. Prior to 8.5.0, 8.4.2, 8.3.4, 8.2.4, 8.1.5, 8.0.6, 7.13.8, and 7.10.12, in the visitors.info endpoint, https://developer.rocket.chat/apidocs/get-visitor-information-by-id-1, token is returned in the response. It looks like there's no use case for the token to be present in the response and it would be a good security practice to remove it altogether. This vulnerability is fixed in 8.5.0, 8.4.2, 8.3.4, 8.2.4, 8.1.5, 8.0.6, 7.13.8, and 7.10.12.	2026-06-24	6.7	CVE-2026-49278
RocketChat--Rocket.Chat	Rocket.Chat is an open-source, secure, fully customizable communications platform. Prior to 8.5.0, the ImageElement component in packages/gazzodown renders user-controlled src values directly into <a href> and attributes without protocol sanitization. Unlike the analogous LinkSpan component - which uses sanitizeUrl to block javascript:, data:, and vbscript: protocols - ImageElement passes the raw URL through unchanged. An authenticated user can post a markdown image with a javascript: URL that, if clicked on an older browser, would execute arbitrary JavaScript in the viewer's session. This vulnerability is fixed in 8.5.0.	2026-06-24	4.4	CVE-2026-47733
Roxnor--GetGenie	Subscriber Sensitive Data Exposure in GetGenie <= 4.4.2 versions.	2026-06-26	6.5	CVE-2026-57316
rtk-ai--rtk	@rtk-ai/rtk-rewrite transparently rewrites shell commands executed via OpenClaw's exec tool to their RTK equivalents. In 1.0.0, the @rtk-ai/rtk-rewrite OpenClaw plugin passes attacker-controlled input directly into a shell-backed execSync() template string without shell-safe escaping. JSON.stringify() wraps the value in double quotes and escapes inner double-quotes and backslashes, but leaves \$() and backtick shell metacharacters untouched. Because execSync delegates execution to /bin/sh -c, the shell expands \$(...) substitutions even inside double-quoted strings, causing the injected subcommand to execute before rtk is invoked. An attacker who can influence the exec tool's command parameter (e.g., via an LLM agent prompt or gateway/tool-call input) achieves arbitrary OS command execution with the privileges of the plugin/gateway process.	2026-06-23	6.3	CVE-2026-55249

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rustfs--rustfs	RustFS is a distributed object storage system built in Rust. In 1.0.0-beta.7 and earlier, the real-time metrics endpoint at /rustfs/admin/v3/metrics is accessible to any valid IAM user regardless of their assigned policy. Every other admin handler in the codebase calls validate_admin_request to enforce admin-action IAM checks; the MetricsHandler skips this call entirely. A restricted IAM user whose policy grants only access to their own bucket can read server-wide operational metrics including disk I/O statistics, network throughput, scanner cycle timing, and cluster RPC state.	2026-06-26	4.3	CVE-2026-55838
samuelclay--NewsBlur	NewsBlur before 14.5.0 contains a broken access control vulnerability that allows authenticated users to read private notification feeds by supplying arbitrary user_id values to the GET /social/interactions endpoint without ownership verification. Attackers can enumerate user_id values to access another user's follows, replies, and social activity without authorization.	2026-06-25	4.3	CVE-2026-56772
secufor--Secufor_OAuth	The Secufor_OAuth plugin for WordPress is vulnerable to unauthorized access in all versions up to, and including, 1.0.7. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to disconnect the WordPress site from its linked Secufor account by clearing the plugin's stored login token and user login configuration.	2026-06-24	5.3	CVE-2026-7617
SeedProd LLC.--SeedProd Pro	Contributor Cross Site Scripting (XSS) in SeedProd Pro < 6.19.5 versions.	2026-06-26	6.5	CVE-2026-57617
seo_tools--Bulk SEO Image	The Bulk SEO Image plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to and including 1.1. This is due to missing or incorrect nonce validation on the plugin's settings page handler BulkSeoImage(), which dispatches to launchbulk() / BulkSeoImageGo() whenever the request contains \$_POST['bulkseoimage']. No wp_nonce_field() is emitted in the form and no check_admin_referer()/wp_verify_nonce() is performed before bulk-overwriting the _wp_attachment_image_alt post meta for every image attached to every published post and/or page. This makes it possible for unauthenticated attackers to bulk-overwrite image ALT-text metadata across the site via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-24	4.3	CVE-2026-11997
SEOPress Free--SEOPress PRO	Contributor Broken Access Control in SEOPress PRO <= 9.1.1 versions.	2026-06-26	4.3	CVE-2026-57430
Shenzhen i365-Tech Co. Ltd.--Setracker2 Parental Control App (Android) package com.tgelec.setracker	Setracker2 Android Companion App com.tgelec.setracker versions 3.1.5 and prior have a predictable registration ID derived from IMEI. The enrollment system lacks additional authentication before assignment. If an attacker is able to obtain the registration ID, they would be able to arbitrarily enroll watches belonging to other users.	2026-06-25	6.5	CVE-2026-9219
ShortPixel--ShortPixel Adaptive Images	Unauthenticated Arbitrary File Deletion in ShortPixel Adaptive Images <= 3.11.4 versions.	2026-06-26	5.8	CVE-2026-56066

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Significant-Gravitas--AutoGPT	AutoGPT is a workflow automation platform for creating, deploying, and managing continuous artificial intelligence agents. Prior to , the `POST /api/integrations/webhooks/{webhook_id}/ping` endpoint fetches the target webhook by primary key alone without verifying that the webhook belongs to the authenticated user. Any authenticated user can supply an arbitrary webhook_id to confirm webhook existence, leak the webhook's OAuth provider type, and in some cases trigger a ping delivery on behalf of another user. This vulnerability is fixed in .	2026-06-26	5.4	CVE-2026-56823
SiteGround--SiteGround Email Marketing	Unauthenticated Broken Access Control in SiteGround Email Marketing <= 1.7.5 versions.	2026-06-26	5.3	CVE-2026-24547
siyuan-note--siyuan	SiYuan is an open-source personal knowledge management system. Prior to 3.7.0, the /api/icon/getDynamicIcon endpoint is explicitly excluded from authentication in SiYuan's kernel router (router.go, "ä¸­éœ€èé%´æ¸" - no auth needed). When called with type=8 and a valid block id parameter, this endpoint invokes RenderDynamicIconContentTemplate, which executes a Go template that includes the querySQL and queryBlocks functions. These functions run arbitrary SELECT statements against the SiYuan SQLite database. An unauthenticated network-adjacent attacker who knows a valid block ID can exfiltrate all user note content, tags, asset references, and block attributes from the database. This vulnerability is fixed in 3.7.0.	2026-06-24	5.9	CVE-2026-54068
StatCounter--StatCounter	Contributor Cross Site Scripting (XSS) in StatCounter <= 2.1.1 versions.	2026-06-26	6.5	CVE-2026-57629
studiowombat--Shoppable Images Lite	Subscriber Broken Access Control in Shoppable Images Lite <= 1.3 versions.	2026-06-26	4.3	CVE-2026-57649
Stylemix--MasterStudy LMS	Subscriber Broken Access Control in MasterStudy LMS <= 3.7.30 versions.	2026-06-26	4.3	CVE-2026-57640
surbma--Surbma Infusionsoft Shortcode	The Surbma Infusionsoft Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'infusionsoft-form' shortcode in versions up to, and including, 2.0.1. This is due to insufficient input sanitization and output escaping on user-supplied 'account' and 'id' shortcode attributes in the surbma_infusionsoft_shortcode_shortcode() function, which are concatenated directly into a <script> tag's src attribute. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-27	6.4	CVE-2026-11597
SureCart--SureCart	Subscriber Cross Site Scripting (XSS) in SureCart <= 4.2.2 versions.	2026-06-26	6.5	CVE-2026-57313
templatescodert-hemes--Spexo	The Spexo theme for WordPress is vulnerable to unauthorized access due to a missing capability check on the activate_plugin function in all versions up to, and including, 2.0.11. This makes it possible for authenticated attackers, with Subscriber-level access and above, to activate a limited set of plugins.	2026-06-27	4.3	CVE-2026-12471

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenable--Nessus	A SQL injection vulnerability in Nessus allows a remote, unauthenticated attacker who controls reverse DNS records for a scanned host to inject malicious SQL into the scan results database, potentially enabling exfiltration of scan-result data.	2026-06-25	5.3	CVE-2026-57587
Themegrill--User Registration	Unauthenticated Broken Access Control in User Registration <= 5.2.2 versions.	2026-06-26	6.5	CVE-2026-52701
Themeisle--Neve PRO	Contributor Cross Site Scripting (XSS) in Neve PRO <= 3.1.2 versions.	2026-06-26	6.5	CVE-2026-57618
Themeisle--PPOM for WooCommerce	Improper Access Control vulnerability in Themeisle PPOM for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects PPOM for WooCommerce: from n/a through 33.0.18.	2026-06-25	6.5	CVE-2026-56050
themeisle--Stripe Payment Forms by WP Full Pay Accept Credit Card Payments, Donations & Subscriptions	The WP Full Stripe Free plugin for WordPress is vulnerable to Missing Authorization in versions up to, and including, 8.4.3 via the wpfs_update_failed_payment_status AJAX action. The handler is registered through both wp_ajax_ and wp_ajax_nopriv_ hooks and the underlying update_failed_payment_status() function performs no capability check, no nonce verification, and no logged-in check before calling \$this->db->updatePaymentByEventId() with attacker-controlled POST parameters. This makes it possible for unauthenticated attackers who can obtain a valid Stripe Payment Intent ID for the target site (Payment Intent IDs are exposed to the customer browser during normal Stripe.js checkout flows) to manipulate payment records in the site's database, marking previously successful payments as failed and overwriting failure codes and messages with attacker-supplied values.	2026-06-27	5.3	CVE-2026-12432
Themeum--Kirki	Subscriber Server Side Request Forgery (SSRF) in Kirki <= 6.0.11 versions.	2026-06-26	4.9	CVE-2026-57627
Tim Strifler--Exclusive Addons Elementor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tim Strifler Exclusive Addons Elementor allows Stored XSS. This issue affects Exclusive Addons Elementor: from n/a through 2.7.9.8.	2026-06-26	6.5	CVE-2026-57620
tomojitakasu--RTKLIB	RTKLIB through 2.4.3 contains an off-by-one out-of-bounds read vulnerability in the decode_ssr3 function at src/rbcm3.c:1446 that allows remote attackers to trigger a global buffer overflow via crafted RTCM3 SSR messages with attacker-controlled signal mode fields. Remote attackers can exploit this vulnerability by sending malicious SSR correction streams over NTRIP or serial connections to cause denial of service or crash RTKLIB rovers and CORS servers.	2026-06-25	6.5	CVE-2026-56787
tomojitakasu--RTKLIB	RTKLIB through 2.4.3 contains a heap buffer overflow vulnerability in the readrxobsb function in src/rinex.c that allows attackers to trigger memory corruption by failing to clamp satellite count values from RINEX epoch headers. Attackers can craft malicious RINEX files declaring more than 64 satellites per epoch to cause heap buffer overflow writes and out-of-bounds stack reads, crashing RTKLIB-based applications including rxn2rtkp and RTKPOST.	2026-06-25	6.5	CVE-2026-56789
tomojitakasu--RTKLIB	RTKLIB through 2.4.3 contains an out-of-bounds read vulnerability in getcodepri function when processing unrecognized RINEX observation	2026-06-25	4.4	CVE-2026-56788

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	codes, allowing attackers to trigger denial of service. Crafted RINEX files with unknown observation types cause negative array indexing into the codepris table, resulting in reliable crashes and potential memory disclosure of adjacent global data.			
ToolJet--ToolJet	ToolJet is the open-source foundation am AI-native platform for building and deploying internal tools, workflows and AI agents. Prior to 3.20.1780-lts, the authenticated endpoint POST /api/data-sources/decrypt returns the decrypted plaintext for any credential whose credential_id is supplied in the request body. Unlike every neighbouring data-source route, this handler is not protected by ValidateDataSourceGuard, does not receive the calling @User(), and the underlying CredentialsService.getValue() looks the credential up by id only, with no organization scoping. As a result, any authenticated user of any organization can decrypt the data-source secrets of any other organization by supplying that organization's credential_id - a cross-tenant confidentiality breach. This vulnerability is fixed in 3.20.1780-lts.	2026-06-25	6.8	CVE-2026-55411
TortoiseGit team--TortoiseGit	Argument Injection in TortoiseGitBlame via Malicious Git History Filenames Leads to Arbitrary File Write in TortoiseGit	2026-06-24	5.5	CVE-2026-11968
trainingbusiness pros--Groundhogg CRM, Newsletters, and Marketing Automation	The Groundhogg - CRM, Newsletters, and Marketing Automation plugin for WordPress is vulnerable to generic SQL Injection via the 'after' parameter in all versions up to, and including, 4.5.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Sales Manager-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The AJAX handler wp_ajax_groundhogg_get_contacts_table has its capability check commented out and performs no nonce verification, meaning any authenticated user regardless of role can reach the vulnerable code path.	2026-06-26	6.5	CVE-2026-13226
trainingbusiness pros--Groundhogg CRM, Newsletters, and Marketing Automation	The Groundhogg - CRM, Newsletters, and Marketing Automation plugin for WordPress is vulnerable to generic SQL Injection via the 'search' parameter in all versions up to, and including, 4.5.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with marketer-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-06-27	6.5	CVE-2026-13331
trainingbusiness pros--Groundhogg CRM, Newsletters, and Marketing Automation	The Groundhogg - CRM, Newsletters, and Marketing Automation plugin for WordPress is vulnerable to generic SQL Injection via 'query[select]' Parameter in all versions up to, and including, 4.5.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Sales Representative-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The sanitized Contact_Query code path can be bypassed by supplying an invalid filter type (e.g., query[filters][0][0][type]=invalid_filter_nonexistent), causing a	2026-06-27	6.5	CVE-2026-13333

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	FilterException to be caught and execution to fall through to the unsanitized Legacy_Contact_Query path.			
TryGhost--Ghost	Ghost is a Node.js content management system. From 6.0.9 until 6.21.1, when making an external request, it is possible to bypass the IP filter that ensures the request isn't going to an internal service using an IPv6 literal which maps to a private IPv4 address. This vulnerability is fixed in 6.21.1.	2026-06-24	5.8	CVE-2026-53944
TryGhost--Ghost	Ghost is a Node.js content management system. From 6.19.4 until 6.21.1, when re-rendering posts, Ghost would refetch missing image dimensions by issuing an outbound HTTP request to the URL stored on an image card - without restricting that URL to trusted image hosts. An authenticated staff user able to create or edit posts could therefore point an image card at an attacker-chosen host and cause the Ghost server to request it on their behalf, including hosts on internal networks or cloud instance metadata endpoints that would not normally be reachable from the public internet. This vulnerability is fixed in 6.21.1.	2026-06-24	5.4	CVE-2026-53946
TryGhost--Ghost	Ghost is a Node.js content management system. From 5.18.0 until 6.21.1, a discrepancy in responses from the members signin endpoints made it possible for an unauthenticated attacker to determine whether a given email address belongs to a registered member of a Ghost site. This vulnerability is fixed in 6.21.1.	2026-06-24	5.3	CVE-2026-53947
TryGhost--Ghost	Ghost is a Node.js content management system. From 6.19.4 until 6.21.1, insufficient validation of the client-supplied Content-Type on Ghost's Admin API file upload endpoint allowed uploaded files to be served from the site with an attacker-chosen content type on S3/GCS storage backends. On installations that serve uploaded files from the same origin as the site, this could have been used to facilitate stored cross-site scripting against site visitors or staff. This vulnerability is fixed in 6.21.1.	2026-06-24	5.4	CVE-2026-53948
TryGhost--Ghost	Ghost is a Node.js content management system. From 5.46.1 until 6.21.2, the validation applied to filters on the public API endpoints could be partially bypassed, making it possible to reveal private fields via a brute force attack. If SQLite was used as the database password hashes were fully accessible. If MySQL was used as the database the password hashes' case (uppercase / lowercase) would have been lost, which would likely have rendered a further brute force attack on the discovered hashes fruitless. This vulnerability is fixed in 6.21.2.	2026-06-24	5.3	CVE-2026-53949
TryGhost--Ghost	Ghost is a Node.js content management system. From 6.0.9 until 6.21.1, Ghost's private-IP check for outbound HTTP requests could be bypassed via DNS rebinding, allowing an attacker to coerce the Ghost server into reaching hosts on internal networks through features that issue external fetches. This vulnerability is fixed in 6.21.1.	2026-06-24	4	CVE-2026-53945
tychesoftware--Abandoned Cart Lite for WooCommerce	Unauthenticated Cross Site Request Forgery (CSRF) in Abandoned Cart Lite for WooCommerce <= 6.8.0 versions.	2026-06-26	4.3	CVE-2026-57637
tychesoftware--Payment Gateway Based Fees and	Unauthenticated Insecure Direct Object References (IDOR) in Payment Gateway Based Fees and Discounts for WooCommerce <= 3.0.0 versions.	2026-06-26	6.5	CVE-2026-56048

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Discounts for WooCommerce				
ueberdosis-- tiptap-php	Tiptap for PHP before version 2.1.1 contains an input validation vulnerability that allows authenticated attackers to cause a denial of service by submitting Tiptap JSON with the attrs.href field set to an array instead of a string, causing an unhandled TypeError in the Link::isAllowedUri() function when passed to preg_match(). Attackers can persist malformed JSON records that permanently crash the server-side HTML rendering pipeline for all subsequent viewers of that record until the database entry is manually repaired.	2026-06-24	6.5	CVE-2026-47110
ultrajson-- ultrajson	UltraJSON is a fast JSON encoder and decoder written in pure C with bindings for Python 3.7+. Prior to 5.13.0, ujson.dumps() (or ujson.dump() or ujson.encode()) have a reject_bytes=False option. When set, they may accept malformed or truncated UTF-8 byte sequences, silently rewriting them into different Unicode characters instead of rejecting them. This leads to input validation bypass and data integrity issues. This vulnerability is fixed in 5.13.0.	2026-06-22	6.5	CVE-2026-54911
verenigingvanreg-- istrars--Generate Security.txt	The Generate Security.txt plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.0.12. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete the site's security.txt file from the server filesystem or create the .well-known directory by directly invoking the delete_securitytxt or create_wellknown_folder AJAX actions.	2026-06-24	4.3	CVE-2026-9616
VillaTheme-- Bopo WooCommerce Product Bundle Builder	Unauthenticated Sensitive Data Exposure in Bopo - WooCommerce Product Bundle Builder <= 1.1.6 versions.	2026-06-26	4.3	CVE-2026-57664
VillaTheme-- GIFT4U	Unauthenticated Broken Access Control in GIFT4U <= 1.0.10 versions.	2026-06-26	6.5	CVE-2026-57324
vim--vim	Vim is an open source, command line text editor. From 9.1.1784 until 9.2.0678, when the bundled zip plugin autoload/zip.vim falls back to PowerShell to browse, read, extract, update or delete entries in a zip archive, it builds the PowerShell command by inserting archive entry names that are quoted only for the shell, not for PowerShell. A crafted entry name can break out of the intended string context and cause PowerShell to execute arbitrary commands with the privileges of the user running Vim, triggered by opening, viewing or extracting the archive. This vulnerability is fixed in 9.2.0678.	2026-06-25	6.5	CVE-2026-57453
vim--vim	Vim is an open source, command line text editor. Prior to 9.2.0662, the dump_prefixes() function in src/spell.c walks a spell-file prefix trie iteratively with a depth counter while dumping the prefixes that apply to a word. The counter is bounded only by the trie structure itself; it is never checked against the size of the fixed MAXWLEN-element stack arrays it indexes (prefix[], arridx[], curi[]). A crafted .spl file, loaded when the user dumps the word list, can drive the descent arbitrarily deep, so the function writes past the end of those arrays. This is a stack out-of-bounds write that	2026-06-25	5.5	CVE-2026-55892

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	corrupts the call frame and crashes the editor. This vulnerability is fixed in 9.2.0662.			
vim--vim	Vim is an open source, command line text editor. Prior to 9.2.0670, get_text_props() in src/textprop.c reads a uint16 property count stored inline after a line's text and returns it as the number of 32-byte textprop_T entries that follow. The only check is a floor that guarantees room for a single entry; the count is never checked against the amount of data actually present. A line that declares a large count while carrying little data causes consumers to read far past the end of the line buffer. Such a line can be delivered through a crafted undo file, leading to a crash. This vulnerability is fixed in 9.2.0670.	2026-06-25	5.3	CVE-2026-57451
vim--vim	Vim is an open source, command line text editor. Prior to 9.2.0671, when Vim opens a file encrypted with the VimCrypt~04! or VimCrypt~05! method (xchacha20poly1305, requires the +sodium feature) whose body is shorter than a single libsodium secretstream header, an unsigned length calculation underflows and a subsequent decryption call reads far past the end of the input buffer, crashing Vim. This vulnerability is fixed in 9.2.0671.	2026-06-25	5.5	CVE-2026-57452
vinod-dalvi--Ivory Search WordPress Search Plugin	The Ivory Search - WordPress Search Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'menu_title' and 'menu_magnifier_color' Settings in all versions up to, and including, 5.5.15 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-27	4.4	CVE-2026-11356
vllm-project--vllm	vLLM is an inference and serving engine for large language models (LLMs). Prior to 0.22.0, vLLM's revision pinning controls do not consistently apply to all artifacts loaded for a model. A deployment that supplies --revision or --code-revision can still load dynamic code, GGUF files, image processors, retrieval side weights, or same-repository subfolder weights/config from an unpinned/default revision. This is a supply-chain integrity issue for pinned vLLM deployments. Operators can believe they are serving a reviewed model revision while vLLM resolves behavior-affecting nested or sibling artifacts outside that reviewed revision. This vulnerability is fixed in 0.22.0.	2026-06-22	6.5	CVE-2026-47155
vllm-project--vllm	vLLM is an inference and serving engine for large language models (LLMs). Prior to 0.23.1rc0, vLLM's /v1/audio/transcriptions endpoint limits compressed upload size but not decoded PCM output. A 25MB OPUS file expands to ~14.9GB of float32 PCM at decode time. This vulnerability is fixed in 0.23.1rc0.	2026-06-22	6.5	CVE-2026-54233
vllm-project--vllm	vLLM is an inference and serving engine for large language models (LLMs). Prior to 0.23.1rc0, the fix for CVE-2026-22778, which introduced a sanitize_message helper that strips object-repr memory addresses from error messages before they reach the client, is incomplete: several response paths echo str(exc) directly to clients without calling sanitize_message. The unsanitized sites include the Anthropic API router in vllm/entrypoints/anthropic/api_router.py (the POST /v1/messages and POST /v1/messages/count_tokens handlers), the Server-Sent Events streaming converter in vllm/entrypoints/anthropic/serving.py, and the realtime speech-to-text WebSocket in	2026-06-22	5.3	CVE-2026-54236

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vllm/entrypoints/speech_to_text/realtime/connection.py. These paths catch the exception inside the route coroutine and construct the JSONResponse themselves, bypassing the sanitizing global FastAPI exception handler, and WebSocket frames do not traverse that handler chain at all. Using the same primitive as the parent issue, an unauthenticated attacker can send malformed image bytes through the Anthropic Messages API image content parts so that PIL.Image.open raises an UnidentifiedImageError whose message contains the BytesIO object repr, leaking the heap memory address verbatim in the error.message field of the response body. This vulnerability is fixed in 0.23.1rc0.			
volcengine--OpenViking	A vulnerability was detected in volcengine OpenViking up to 0.3.21. This affects the function str_to_uint64 of the file openviking/storage/vectordb/utis/str_to_uint64.py of the component Local VectorDB Primary-key Label Handler. The manipulation of the argument ID results in insufficient verification of data authenticity. The attack may be launched remotely. Attacks of this nature are highly complex. The exploitability is reported as difficult. The pull request to fix this issue awaits acceptance.	2026-06-28	5	CVE-2026-13507
warpdotdev--warp	Warp is an agentic development environment. From 0.2021.04.25.23.05.stable_00 until 0.2026.05.06.15.42.stable_01, Warp accepted certain state-mutating terminal lifecycle hooks from the PTY stream without verifying that the hooks were emitted by Warp's shell integration for the active session. An attacker who could cause a victim to view attacker-controlled terminal output in Warp could spoof selected lifecycle metadata, including the current working directory reported for the active block or SSH session transport metadata. This vulnerability is fixed in 0.2026.05.06.15.42.stable_01.	2026-06-24	4.3	CVE-2026-54686
WCBoost--WCBoost Products Compare	Unauthenticated Sensitive Data Exposure in WCBoost – Products Compare <= 1.1.0 versions.	2026-06-26	5.3	CVE-2026-57633
webaways--NEX-Forms Ultimate Forms Plugin for WordPress	The NEX-Forms - Ultimate Forms Plugin for WordPress plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 9.2.2. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to enumerate sequential report IDs and download complete form submission data - including names, email addresses, phone numbers, postal addresses, payment details, and uploaded file paths - for any saved report on the site.	2026-06-27	5.3	CVE-2026-12404
wedevs--Dokan Pro	The Dokan Pro plugin for WordPress is vulnerable to time-based SQL Injection via the 'orderby' parameter in all versions up to, and including, 5.0.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-06-25	6.5	CVE-2026-12079
withastro--astro	@astrojs/netlify is an adapter that allows Astro to deploy your hybrid or server rendered site to Netlify. Prior to 7.0.13, @astrojs/netlify converts Astro image.remotePatterns into Netlify Image CDN	2026-06-22	5.3	CVE-2026-54300

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	images.remote_images regular expressions with broader semantics than Astro's canonical matcher. A single wildcard hostname such as *.example.com is converted to an optional subdomain regex, so the apex host matches. A single wildcard pathname such as /ok/* is converted without end anchoring, so deeper paths match by prefix. This vulnerability is fixed in 7.0.13.			
withastro--astro	Astro is a web framework. Prior to 6.4.6, the spreadAttributes function in Astro's server-side rendering pipeline iterates over object keys and passes them directly to addAttribute, which interpolates the key into the HTML output without escaping. When a developer uses the spread syntax {...props} on an HTML element and the object keys come from an untrusted source (API, CMS, URL parameters), an attacker can inject arbitrary HTML attributes including event handlers like onmousemove, onclick, or break out of the attribute context entirely to inject new elements. This vulnerability is fixed in 6.4.6.	2026-06-22	4.2	CVE-2026-54298
WP Folio Team--PPWP	Contributor Insecure Direct Object References (IDOR) in PPWP <= 1.9.19 versions.	2026-06-26	4.3	CVE-2026-57634
wp.insider--Affiliates Manager	Affiliate Broken Access Control in Affiliates Manager <= 2.9.49 versions.	2026-06-26	6.5	CVE-2026-57654
wpdevteam--Gutenberg Essential Blocks Page Builder for Gutenberg Blocks & Patterns	The Gutenberg Essential Blocks - Page Builder for Gutenberg Blocks & Patterns plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'configurablePrefix' Block Attribute in all versions up to, and including, 6.1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-25	6.4	CVE-2026-10833
wpeverest--User Registration & Membership Free & Paid Memberships, Subscriptions, Content Restriction, User Profile, Custom User Registration & Login Builder	The User Registration & Membership - Free & Paid Memberships, Subscriptions, Content Restriction, User Profile, Custom User Registration & Login Builder plugin for WordPress is vulnerable to unauthorized modification of data due to missing validation checks in the confirm_payment() function in all versions up to, and including, 5.2.0. This makes it possible for unauthenticated attackers to bypass payment processing and activate paid memberships.	2026-06-26	6.5	CVE-2026-1869
WPManageNinja LLC--Fluent Booking	Contributor Cross Site Scripting (XSS) in Fluent Booking <= 2.1.0 versions.	2026-06-26	6.5	CVE-2026-57638
wummel--patool	Patool before 4.0.5 contains a path traversal vulnerability in the safe_extract() function in patoolib/programs/py_tarfile.py when running on Python before 3.12, where the is_within_directory() helper uses os.path.commonprefix() for character-level string comparison instead of path-level comparison, allowing a crafted archive member path to bypass the containment check. Attackers can supply a malicious archive with specially crafted member paths to write arbitrary files.	2026-06-26	5.4	CVE-2026-29509

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xpro--Xpro Addons 140+ Widgets for Elementor	The Xpro Addons - 140+ Widgets for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'custom_attributes' parameter in all versions up to, and including, 1.7.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-06-24	6.4	CVE-2026-11614
yapacdev--WhatsOrder Instant Checkout for WooCommerce	The WhatsOrder - Instant Checkout for WooCommerce plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.0.1 via the yapacdev_generate_order_pdf. This makes it possible for unauthenticated attackers to extract sensitive customer PII and order details - including full name, email address, phone number, billing address, ordered items with quantities and prices, applied coupons, shipping method, and order total - from any customer's invoice by enumerating sequential order IDs. Invoice HTML files are written to the publicly accessible wp-content/uploads/whatsorder_invoices/ directory, which is created without an .htaccess deny rule or index.php guard, making every invoice directly downloadable over HTTP with no authentication check.	2026-06-24	5.3	CVE-2026-9612
yashpokharna2555--restaurent-management-system	A security flaw has been discovered in yashpokharna2555 restaurent-management-system. This impacts an unknown function of the file login_register.php of the component Registration Handler. Performing a manipulation of the argument Username results in cross site scripting. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-28	4.3	CVE-2026-13499
yt-dlp--yt-dlp	yt-dlp is a command-line audio/video downloader. From 2023.09.24 until 2026.06.09, if curl is used as an external downloader for yt-dlp, cookies may be leaked to an unintended host upon HTTP redirect or when the host for download fragments differs from their parent manifest's. At the file download stage, the cookies are passed by yt-dlp to the file downloader via --cookie. However, unless these are loaded from a file, this operation does not activate the cookie engine. As a result, curl will send cookies with requests to domains or paths for which the cookies are not scoped. This vulnerability is fixed in 2026.06.09.	2026-06-23	6.1	CVE-2026-50019
zephyrproject--zephyr	The Zephyr Bluetooth LE Audio Basic Audio Profile (BAP) unicast client mishandles peer-supplied ASE state notifications. In unicast_client_ep_qos_state() (subsys/bluetooth/audio/bap_unicast_client.c), the handler writes attacker-controlled QoS fields (interval, framing, phy, sdu, rtn, latency, pd) through the stream-qos pointer with only a stream != NULL guard. stream-qos is NULL for any stream that has been codec-configured via bt_bap_stream_config() but not yet added to a unicast group (it is set only by unicast_group_add_stream()). A malicious or buggy remote ASCS server, to which the local device is connected as a BAP unicast client, can send a GATT notification announcing the ASE has entered the QoS Configured state while the local endpoint is still in the Codec Configured state - a transition the dispatcher explicitly permits - during that window,	2026-06-28	6.5	CVE-2026-10593

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	causing a write through a NULL pointer and a crash (denial of service). The data written is itself remote-controlled. The defect shipped in v4.3.0 and v4.4.0 (and earlier). The fix re-points all BAP QoS storage to the always-valid embedded ep-qos struct, eliminating the NULL dereference.			
zephyrproject--zephyr	The Zephyr PL011 UART driver (drivers/serial/uart_pl011.c) contains an unbounded software loop in pl011_irq_tx_enable() that repeatedly invokes the interrupt-driven application callback while the TX interrupt mask bit (PL011_IMSC_TXIM) is set, to work around the controller's level-transition TX-interrupt behavior. When CTS hardware flow control is enabled (devicetree hw-flow-control or runtime UART_CFG_FLOW_CTRL_RTS_CTS) and the wired serial peer de-asserts CTS, the controller stops draining the TX FIFO; pl011_fifo_fill() then returns 0 on every call while the application still has pending data and therefore never disables the TX interrupt. The loop condition never clears, so the thread that called uart_irq_tx_enable() (e.g. h4_send() in the Bluetooth HCI H4 driver) spins indefinitely, hanging the executing context and stalling the transport - a denial of service (CWE-835). An attacker controlling the device attached to the UART's CTS line can trigger the hang by withholding CTS during transmission. Impact is availability only; there is no memory-safety, confidentiality, or integrity consequence. The vulnerable loop was introduced in commit b783bc8448ef (Feb 2025) and shipped in releases v4.1.0 through v4.4.0. The fix breaks out of the loop when CTS is blocking and arms the CTS modem-status interrupt to resume transmission when CTS re-asserts.	2026-06-24	6.5	CVE-2026-10642
zephyrproject--zephyr	The Microchip SERCOM-G1 UART driver (drivers/serial/uart_mchp_sercom_g1.c), used by the PIC32CM-JH SoC family, contains an out-of-bounds write in its asynchronous (DMA) receive path. When uart_rx_enable() is invoked with a one-byte receive buffer (len == 1) and CONFIG_UART_MCHP_ASYNC is enabled, the RX-complete ISR starts a single-beat DMA transfer while a received byte is already pending in the SERCOM DATA register. On this SoC the peripheral-triggered DMA start sequencing then writes one byte past the end of the caller-supplied buffer (CWE-787). The overflowed byte's value is the UART RX data supplied by the connected serial peer (adjacent attacker), while its size and location are fixed at one byte immediately after the buffer. Exploitation requires the async UART config (not enabled by default on the in-tree PIC32CM-JH boards) and a consumer that enables RX with a one-byte buffer; impact is limited single-byte memory corruption adjacent to the RX buffer (possible crash / denial of service). The defect shipped in v4.4.0. The fix reads the first byte with the CPU and, for one-byte buffers, performs no DMA at all; for larger buffers it sizes the DMA for the remaining len-1 bytes.	2026-06-28	4.2	CVE-2026-10644
zephyrproject--rtos--Zephyr	Zephyr's ext2 directory-entry parser does not fully validate on-disk directory entry structure before copying the entry name and advancing traversal state. In ext2_fetch_direntry() (subsys/fs/ext2/ext2_diskops.c), the code only checks de_name_len <= EXT2_MAX_FILE_NAME and then copies the name with memcpy without validating the structural relationship between de_rec_len, de_name_len, and the directory block boundary (for example that de_rec_len is non-zero, at least the size of the entry header, and that the record fits within the block). Callers such as find_dir_entry() and ext2_get_direntry() (subsys/fs/ext2/ext2_impl.c) then	2026-06-22	4.9	CVE-2026-10645

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	advance traversal using the unvalidated de_rec_len. A crafted ext2 image can therefore cause an out-of-bounds read from the directory block buffer when a malformed entry near the end of a block triggers an oversized name copy, or a zero-progress infinite loop when de_rec_len == 0. The issue is not reached at mount time but later through directory traversal paths such as pathname lookup, stat/open/unlink/rename, and readdir. The primary impact is denial of service and out-of-bounds reads under attacker-controlled ext2 images mounted from untrusted media.			
666ghj--BettaFish	A vulnerability was determined in 666ghj BettaFish up to 1.2.1. Impacted is the function _deduplicate_results of the file InsightEngine/agent.py of the component InsightEngine search-result Deduplication. Executing a manipulation can lead to partial string comparison. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The pull request to fix this issue awaits acceptance.	2026-07-05	5.3	CVE-2026-14687
acl project--acl	acl before version 2.4.0 contains a time-of-check to time-of-use (TOCTOU) race condition vulnerability that allows local attackers to escalate privileges by replacing a pathname component with a symbolic link between an lstat() check and subsequent symlink-following operations such as stat(), chown(), chmod(), acl_get_file(), and acl_set_file(). Attackers who control a pathname component can redirect file access control list operations to arbitrary files when getfacl, setfacl, or chacl is invoked by a privileged process over an attacker-controlled path, resulting in local privilege escalation.	2026-06-29	6.3	CVE-2026-54370
AD-Security--AD_Miner	A vulnerability was determined in AD-Security AD_Miner 1.9.0. Affected is the function request_a of the file ad_miner/scripts/analyse_cache.py of the component Cache Handler. This manipulation of the argument sys.argv[1] causes deserialization. The attack can only be executed locally. The pull request to fix this issue awaits acceptance.	2026-07-05	5.3	CVE-2026-14723
Addify--Tax Exempt for WooCommerce	Customer Path Traversal in Tax Exempt for WooCommerce <= 1.9.3 versions.	2026-07-02	6.5	CVE-2026-49779
Adobe--ColdFusion	ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to gain limited read and write access to unauthorized files or directories outside the intended restrictions. Exploitation of this issue does not require user interaction.	2026-06-30	6.5	CVE-2026-48314
Ads WPQuads--Ads by WPQuads	Subscriber Broken Access Control in Ads by WPQuads <= 3.0.3 versions.	2026-06-29	6.5	CVE-2026-57335
agentejo--Cockpit CMS	A security vulnerability has been detected in agentejo Cockpit CMS up to 0.12.2. Affected by this issue is the function Spyc::YAMLLoad of the file /config/config.yaml of the component htaccess Handler. Such manipulation leads to files or directories accessible. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. Configuration settings should be changed. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-29	5.3	CVE-2026-13533

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
AIAnytime--Awesome-MCP-Server	A flaw has been found in AIAnytime Awesome-MCP-Server up to a884bb51bcd99e08e14fd712c749d55d9d9a13ab. Affected by this issue is some unknown functionality of the file mcp-wiki/src/mcp_wiki/server.py of the component mcp-wiki/wiki-summary. This manipulation of the argument url causes server-side request forgery. The attack may be initiated remotely. The exploit has been published and may be used. This product uses a rolling release model to deliver continuous updates. As a result, specific version information for affected or updated releases is not available. The project was informed of the problem early through an issue report but has not responded yet.	2026-07-05	6.3	CVE-2026-14748
andrasweb--PixMagix WordPress Image Editor	The PixMagix - WordPress Image Editor plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.7.2 via the move_image_on_server function. This makes it possible for authenticated attackers, with author-level access and above, to write files with attacker-controlled content to arbitrary locations on the server. The unsanitized 'layers[].id' parameter is concatenated into a filesystem path and passed to PHP's copy() function, allowing traversal sequences (e.g. '../..') to escape the intended upload directory and write attacker-supplied file contents to arbitrary paths accessible by the web server process. The save_template REST endpoint is gated by the create_projects permission (edit_pixmagix + upload_files), which Author-level users hold by default after plugin activation, making this exploitable by any Author on sites running PixMagix.	2026-06-30	6.5	CVE-2026-11367
Andrew Fiebert--Simple URLs	Author Cross Site Scripting (XSS) in Simple URLs <= 151 versions.	2026-07-02	5.9	CVE-2026-57762
api-platform--core	API Platform Core is a system to create hypermedia-driven REST and GraphQL APIs. In versions prior to 4.1.30, 4.2.26 and 4.3.12, the serializer's AbstractItemNormalizer does not validate the resource type returned when resolving relation IRIs, allowing type confusion where a resource of an unintended type can be silently assigned to a relation property. An attacker who can submit write requests (POST/PUT/PATCH) to an API Platform endpoint with writable relations can supply a relation IRI pointing to a resource of a different type than the relation's declared class. Because getResourceFromIri() does not pass an \$operation to IriConverter::getResourceFromIri(), the is_a type guard at IriConverter.php:86 is skipped. For untyped relation properties (legacy @var-only style), the wrong-typed object is silently assigned, corrupting invariants and potentially feeding downstream logic that assumes the declared type (CWE-843). For typed properties (modern PHP 8.x), the substitution is blocked by Symfony's PropertyAccessor with an InvalidTypeException. This issue has been fixed in versions 4.1.30, 4.2.26 and 4.3.12.	2026-07-01	6.5	CVE-2026-54164
api-platform--core	API Platform Core is a system to create hypermedia-driven REST and GraphQL APIs. In versions from 2.6.0 prior to 4.1.29, 4.2.26, and 4.3.12, a missing isCacheKeySafe gate in the JSON:API and HAL item normalizers causes a cross-user attribute leak. #[ApiProperty(security: ...)] is evaluated per request to decide whether a property is exposed. The componentsCache arrays in ApiPlatform\JsonApi\Serializer\ItemNormalizer and ApiPlatform\Hal\Serializer\ItemNormalizer are keyed on \$context['cache_key'], which is set unconditionally before delegating to	2026-07-01	5.9	CVE-2026-49858

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the parent normalizer. The component structure (attributes, relationships, links) computed for one request can therefore be reused for a subsequent request whose user has a different set of accessible properties. A user with lower privileges may end up seeing the structure of properties that the security predicate would otherwise have hidden for them. This issue has been fixed in versions 4.1.29, 4.2.26, and 4.3.12.			
AsyncHttpClient-- async-http-client	The AsyncHttpClient (AHC) library allows Java applications to easily execute HTTP requests and asynchronously process HTTP responses. In versions from 2.0.0 prior to 2.16.0 and from 3.0.0.Beta1 prior to 3.0.11, ThreadSafeCookieStore stored a cookie under the value of its Domain attribute without verifying that the responding host is allowed to set a cookie for that domain, leading to a cookie tossing / cookie injection issue. A host the client connects to can therefore plant a cookie scoped to an unrelated domain, and the client will then send that cookie on later requests to that domain. Applications that use a single AsyncHttpClient instance - and thus the default, shared CookieStore - to reach both an attacker-influenced host and a trusted host are impacted. This issue has been fixed in versions 2.16.0 and 3.0.11.	2026-07-01	4	CVE-2026-55688
Averta LTD-- Shortcodes and extra features for Phlox theme	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Averta LTD Shortcodes and extra features for Phlox theme allows DOM-Based XSS. This issue affects Shortcodes and extra features for Phlox theme: from n/a through 2.17.16.	2026-07-01	6.5	CVE-2026-57737
AWS--AWS CLI	Overly permissive file permissions in AWS CLI before 1.44.78 (v1) and 2.34.29 (v2) on Unix-like systems where the umask has not been configured to restrict file permissions (the default on most systems) may allow other local users on the same host to read credentials written by certain CLI subcommands (aws codeartifact login, aws iam create-virtual-mfa-device, aws deploy register). To remediate this issue, users should upgrade to AWS CLI 1.44.78 (v1) or 2.34.29 (v2) or later.	2026-07-01	5.5	CVE-2026-13769
beardev-- JoomSport for Sports: Team & League, Football, Hockey & more	The JoomSport - for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to Missing Authorization to Arbitrary Group Deletion in versions up to, and including, 5.7.8. This is due to a missing capability check in the joomsport_season_groupdel() AJAX handler, which only verifies a nonce before executing a DELETE query on attacker-supplied group IDs. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary JoomSport group records.	2026-07-01	4.3	CVE-2026-12133
beardev-- JoomSport for Sports: Team & League, Football, Hockey & more	The JoomSport - for Sports: Team & League, Football, Hockey & more plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.7.8. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to create arbitrary season groups or modify existing group names, participants, and round-type options. Exploitation requires obtaining the joomsportajaxnonce, which is exposed on frontend pages that render a JoomSport shortcode.	2026-07-02	4.3	CVE-2026-12134
BMC--Control-M/Enterprise Manager	The Control-M/Enterprise Manager uses weak protections for stored hashes of account passwords, potentially allowing offline password recovery attacks if credential data is obtained by an attacker. This	2026-07-01	5.6	CVE-2026-10540

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability affects Control-M/Enterprise Manager unsupported versions 9.0.20.x and potentially earlier unsupported versions			
Capgo--Capgo	Capgo before 12.128.2 allows multiple public channels for the same app and platform to coexist simultaneously, while unnamed /updates requests without defaultChannel implicitly resolve to a single hidden winner channel. An authorized app or channel manager can create ambiguous default update state and silently influence which bundle unnamed clients receive, breaking release routing integrity and predictability.	2026-06-30	6.5	CVE-2026-56328
Capgo--Capgo	Capgo console.capgo.app/login before 12.128.2 accepts access_token and refresh_token in URL query parameters, automatically authenticating users without confirmation. Attackers can craft malicious links to force victims into attacker-controlled sessions, exposing tokens in browser history and logs.	2026-06-30	5.4	CVE-2026-56224
Capgo--Capgo	Capgo before 12.128.2 contains an information disclosure vulnerability in the /private/validate_password_compliance endpoint that returns different error responses for malformed, non-existent, and existing organization IDs. Unauthenticated attackers can enumerate valid organization UUIDs by observing response status codes and error messages, allowing confirmation of organization existence.	2026-06-30	5.3	CVE-2026-56318
Capgo--Capgo	Capgo before 12.128.2 contains an information disclosure vulnerability in the public.invite_user_to_org RPC function that allows unauthenticated attackers to enumerate organization existence by observing distinct error responses. Attackers can call the SECURITY_DEFINDER function with a publishable API key to determine if an organization ID exists based on NO_ORG versus NO_RIGHTS responses, enabling tenant enumeration attacks.	2026-06-30	5.3	CVE-2026-56327
Capgo--Capgo	Capgo before 12.128.2 contains improper error handling in the /private/accept_invitation endpoint that returns HTTP 500 instead of safe 4xx errors when magic_invite_string is invalid. Attackers can trigger this vulnerability using only the public key by submitting malformed magic_invite_string values to cause server errors and leak internal processing details.	2026-06-30	5.3	CVE-2026-56331
Capgo--Capgo	Capgo before 12.128.2 contains a server-side validation bypass vulnerability in organization security settings that allows authenticated org admins to persist invalid security policy state. Attackers can bypass backend validation by directly updating the public.orgs table from the browser, circumventing field-level validation checks for max_apikey_expiration_days and other security-sensitive configuration parameters.	2026-06-30	4.3	CVE-2026-56333
Capgo--Capgo	Capgo before 12.128.2 lacks an UPDATE row-level security policy for the build_requests table, preventing API-key and anonymous access from persisting builder status updates. Attackers can exploit this missing policy to cause build status and error details to remain unpersisted, leaving build_requests rows stuck in pending state with null last_error values.	2026-06-30	4.3	CVE-2026-56334
ccfos--nightingale	Nightingale (n9e) before 9.0.0-beta.2 exposes full datasource configurations, including plaintext database passwords, HTTP bearer tokens, HTTP basic-auth passwords, and mTLS client keys, to any authenticated low-privilege (Standard role) user through POST	2026-06-30	6.5	CVE-2026-58167

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	/api/n9e/datasource/list. The route is registered without an admin authorization gate, unlike the sibling datasource mutation routes, and the open-source DatasourceFilter does not redact secret fields, so the secret-bearing settings, http, and auth objects are serialized in the response. The disclosed credentials enable access to the connected downstream systems.			
ChaN--FatFs	FatFs R0.16 and earlier exhibits a stale dirty-cache skip via unsigned-subtraction wrap in f_read() / f_write() (fp->sect - sect < cc) during interleaved read/write on fragmented filesystems. This maps to CWE-191 (Integer Underflow). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H (6.1, Medium). The estimated CISA SSVS vectors are Exploitation: PoC, Technical Impact: Total.	2026-07-01	6.1	CVE-2026-6685
ChaN--FatFs	FatFs R0.16 and earlier contains a divide-by-zero in exFAT sync logic bug when crafted metadata causes n_fatent - 2 to be zero during write/sync operations. This maps to CWE-369 (Divide By Zero). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H (4.6, Medium). Network-delivered update media can make this remote in some pipelines. The estimated CISA SSVS vectors are Exploitation: PoC, Technical Impact: Partial.	2026-07-01	4.6	CVE-2026-6683
ChaN--FatFs	FatFs prior to R0.16 that use GPT scanning with 'FF_LBA64 = 1' contains an issue where an unbounded loop count derived from GPT header field GPTH_PtNum, enabling extremely long or effectively infinite mount-time scans. This maps to CWE-835 (Loop with Unreachable Exit Condition). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H (4.6, Medium). The estimated CISA SSVS vectors are Exploitation: PoC, Technical Impact: Partial.	2026-07-01	4.6	CVE-2026-6684
ChaN--FatFs	FatFs R0.16 and earlier contains an uninitialized cluster exposure when f_lseek() extends files beyond EOF without zero-filling newly allocated clusters. This maps to CWE-908 (Use of Uninitialized Resource). Estimated CVSS v3.1 vector: CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N (4.6, Medium). The estimated CISA SSVS vectors are Exploitation: PoC, Technical Impact: Partial.	2026-07-01	4.6	CVE-2026-6686
CherryHQ--cherry-studio	A security vulnerability has been detected in CherryHQ cherry-studio up to 1.9.6. This vulnerability affects unknown code of the file src/main/services/mcp/oauth/callback.ts of the component MCP OAuth Local Callback Server. The manipulation of the argument code leads to improper authorization. The attack can be initiated remotely. The attack is considered to have high complexity. It is stated that the exploitability is difficult. The exploit has been disclosed publicly and may be used. The pull request to fix this issue awaits acceptance.	2026-06-29	5.6	CVE-2026-13524
CherryHQ--cherry-studio	A vulnerability was detected in CherryHQ cherry-studio up to 1.9.7. This affects the function sha256 of the file src/main/services/memory/MemoryService.ts of the component CherryIN Preload API. Performing a manipulation of the argument state results in authorization bypass. The attack can be initiated remotely. The attack's complexity is rated as high. It is indicated that the exploitability is difficult. The exploit is now public and may be used. The vendor explains, that "[m]emory is planned to be removed in v2 version."	2026-06-29	5	CVE-2026-13534

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
code-projects--Assessment Management	A flaw has been found in code-projects Assessment Management 1.0. This issue affects some unknown processing of the file /lecturer/marking-scheme.php of the component Database Query Handler. This manipulation of the argument squestions[] causes sql injection. The attack can be initiated remotely. The exploit has been published and may be used.	2026-07-04	6.3	CVE-2026-14657
code-projects--Assessment Management	A vulnerability was detected in code-projects Assessment Management 1.0. This vulnerability affects unknown code of the file /lecturer/marking-scheme.php. The manipulation of the argument smarksrange[] results in sql injection. It is possible to launch the attack remotely. The exploit is now public and may be used.	2026-07-04	6.3	CVE-2026-14658
code-projects--Assessment Management	A security vulnerability has been detected in code-projects Assessment Management 1.0. This affects an unknown part of the file /admin/remove-user.php. The manipulation of the argument ID leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	2026-07-04	4.3	CVE-2026-14656
code-projects--Internship Management System	A vulnerability was detected in code-projects Internship Management System 1.0. This affects an unknown function of the file employer/details/change_password.php of the component Password Change Endpoint. The manipulation of the argument Current results in sql injection. The attack can be executed remotely. The exploit is now public and may be used.	2026-07-05	6.3	CVE-2026-14701
code-projects--Online Examination	A vulnerability was identified in code-projects Online Examination 1.0. This affects an unknown part of the file /update.php?q=addquiz of the component Quiz Creation Feature. The manipulation of the argument name/total/right/wrong/time/tag/desc leads to sql injection. The attack can be initiated remotely. The exploit is publicly available and might be used.	2026-07-05	6.3	CVE-2026-14706
code-projects--Online Music Site	A security flaw has been discovered in code-projects Online Music Site 1.0. This affects an unknown part of the file /Frontend/Feedback.php of the component POST Request Handler. The manipulation of the argument fname/femail/faddress/fmessage results in cross site scripting. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-06-29	4.3	CVE-2026-13567
CodeAstro--Apartment Visitor Management System	A security flaw has been discovered in CodeAstro Apartment Visitor Management System 1.0. The impacted element is an unknown function of the file /apartment-visitor/add-apartment.php. The manipulation of the argument apartmentno results in sql injection. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-07-05	6.3	CVE-2026-14689
CodeAstro--Apartment Visitor Management System	A vulnerability was identified in CodeAstro Apartment Visitor Management System 1.0. Affected by this issue is some unknown functionality of the file /apartment-visitor/search-result.php of the component POST Parameter Handler. The manipulation of the argument searchdata leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	2026-07-05	6.3	CVE-2026-14766
CodeAstro--Complaint	A security flaw has been discovered in CodeAstro Complaint Management System 1.0. The affected element is the function deletereport of the file application/controllers/Report.php of the component Report Endpoint.	2026-06-29	5.4	CVE-2026-13549

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	The manipulation results in authorization bypass. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.			
CodeAstro--Ecommerce Website	A vulnerability has been found in CodeAstro Ecommerce Website 1.0. This impacts an unknown function of the file /ecommerce-website-php/customer/my_account.php?edit_account. Such manipulation of the argument c_name leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2026-07-04	6.3	CVE-2026-14639
CodeAstro--Ecommerce Website	A security flaw has been discovered in CodeAstro Ecommerce Website 1.0. This affects an unknown part of the file /ecommerce-website-php/customer/confirm.php of the component POST Parameter Handler. The manipulation of the argument invoice_no results in sql injection. The attack can be executed remotely. The exploit has been released to the public and may be used for attacks.	2026-07-05	6.3	CVE-2026-14767
CodeAstro--Human Resource Management System	A vulnerability was detected in CodeAstro Human Resource Management System 1.0. This issue affects the function emselectByCode of the file application/models/Employee_model.php of the component Update_Earn_Leave Endpoint. The manipulation of the argument emid results in sql injection. The attack can be launched remotely. The exploit is now public and may be used.	2026-06-29	6.3	CVE-2026-13525
CodeAstro--Human Resource Management System	A flaw has been found in CodeAstro Human Resource Management System 1.0. This vulnerability affects the function GetFileInfo of the file hrsystem/application/models/Employee_model.php of the component View Endpoint. Executing a manipulation of the argument ID can lead to sql injection. The attack can be launched remotely. The exploit has been published and may be used.	2026-06-29	6.3	CVE-2026-13535
CodeAstro--Human Resource Management System	A vulnerability was found in CodeAstro Human Resource Management System 1.0. Impacted is an unknown function. The manipulation results in cross-site request forgery. The attack may be launched remotely. The exploit has been made public and could be used.	2026-06-29	4.3	CVE-2026-13537
codename065--Download Manager	The Download Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'no_data_msg' Shortcode Attribute in all versions up to, and including, 3.3.60 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Although wp_kses_post is applied to post content on save, it only strips HTML tokens and does not neutralize C-style escape sequences embedded within shortcode attribute values, meaning contributors can craft a payload that survives the kses filter and is silently reconstructed into a raw script tag at render time.	2026-07-01	6.4	CVE-2026-13733
codepeople--Appointment Booking Calendar	The Appointment Booking Calendar plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.4.02 via the cpabc_appointments_filter_list. This makes it possible for authenticated attackers, with contributor-level access and above, to extract customer names, email addresses, phone numbers, appointment comments, and other booking personally identifiable information.	2026-07-01	4.3	CVE-2026-12113

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Codexpert Inc--ThumbPress	Missing Authorization vulnerability in Codexpert Inc ThumbPress allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects ThumbPress: from n/a through 6.3.2.	2026-07-01	4.3	CVE-2026-57720
Colissimo--Colissimo Officiel : Mthodes de livraison pour WooCommerce	Unauthenticated Insecure Direct Object References (IDOR) in Colissimo Officiel : MÃ©thodes de livraison pour WooCommerce <= 2.9.0 versions.	2026-06-29	6.5	CVE-2026-57341
coolabsio--coolify	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.464, the executeInDocker() helper wraps commands in bash -c '{command}' without escaping single quotes. User-controlled docker_compose_custom_build_command and docker_compose_custom_start_command fields are interpolated directly, allowing a single quote to break out of the bash -c argument and execute commands on the managed server host (outside the intended Docker container context). This vulnerability is fixed in 4.0.0-beta.464.	2026-06-30	6.6	CVE-2026-27955
coolabsio--coolify	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.464, `GET /api/v1/deployments/{uuid}` in DeployController.php retrieves deployment details without validating that the deployment belongs to the authenticated user's team. Any authenticated API user can read deployment records from other teams by providing a valid deployment UUID. This vulnerability is fixed in 4.0.0-beta.464.	2026-06-30	5	CVE-2026-27881
coolabsio--coolify	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.464, the `GET /api/v1/deployments/{uuid}` endpoint allows any authenticated user to access deployment details belonging to any team, bypassing team-based authorization. The \$teamId is extracted from the authentication token but never used to scope the database query. This vulnerability is fixed in 4.0.0-beta.464.	2026-06-30	5	CVE-2026-27883
coolabsio--coolify	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.461, the GitLab webhook endpoint uses a non-constant-time string comparison operator (!==) to validate the webhook secret token. This implementation is vulnerable to timing attacks, which could allow an attacker to gradually discover the secret token by measuring response time differences. This vulnerability is fixed in 4.0.0-beta.461.	2026-06-30	4.8	CVE-2026-27882
coolabsio--coolify	Coolify is an open-source and self-hostable tool for managing servers, applications, and databases. Prior to 4.0.0-beta.464, `GET /api/v1/servers/{server_uuid}/domains?uuid={app_uuid}` bypasses team scoping when the optional uuid query parameter is provided. Any authenticated API user can enumerate domain names (FQDNs) of applications belonging to other teams. This vulnerability is fixed in 4.0.0-beta.464.	2026-06-30	4.3	CVE-2026-27956
creativemindssol utions--CM Business Directory Optimise and	The CM Business Directory - Optimise and showcase local business plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Business Address Meta Fields in all versions up to, and including, 1.5.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to	2026-07-03	6.4	CVE-2026-8892

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
showcase local business	inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Because the malicious payload is stored in post meta rather than post_content, WordPress's unfiltered_html capability restriction does not apply, meaning contributors who lack that capability can still inject executable HTML via the address meta fields such as cmbd_address, cmbd_cityTown, cmbd_stateCounty, cmbd_postalcode, cmbd_region, and cmbd_country.			
crmp perks-- Database for Contact Form 7, WPforms, Elementor forms	The Database for Contact Form 7, WPforms, Elementor forms plugin for WordPress is vulnerable to Arbitrary File Copy via the create_entry_el() function in versions up to, and including, 1.5.1. The function reads raw_value from Elementor Pro's Form_Record object for upload-type fields and passes it directly to PHP's copy() without validating that the value corresponds to a legitimately uploaded file - when no file is present in \$_FILES, raw_value reflects the attacker-controlled POST string. copy() accepts both local filesystem paths and URL sources, so the attacker can target any file readable by the PHP process or supply an attacker-controlled remote URL. Elementor Pro is a prerequisite for triggering the code path (it owns the elementor_pro/forms/new_record hook and populates the Form_Record object), but the bug itself is entirely in Contact Form Entries' handler. This could allow unauthenticated attackers to disclose arbitrary files on the affected site's server. The file is copied to a directory unknown to the attacker; the hashed directory name provides defense-in-depth but is generated from non-cryptographic sources (uniqid() + rand()) and should not be relied upon as the primary mitigation.	2026-07-02	6.5	CVE-2026-9145
Crocoblock. Jetimpex Inc.-- JetReviews	Subscriber Cross Site Scripting (XSS) in JetReviews <= 3.0.0.1 versions.	2026-07-02	6.5	CVE-2026-57354
cvat-ai--cvat	CVAT before 2.69.0 contains an improper authorization vulnerability in QualityReportViewSet.get_queryset that allows authenticated attackers to enumerate quality report identifiers belonging to other organizations by exploiting a missing check_object_permissions call on the parent_id query parameter of the quality reports API endpoint. Attackers can send requests with sequential integer parent_id values and distinguish between existing and non-existing reports via HTTP 500 versus HTTP 404 response differences, disclosing cross-organization report existence without returning report content.	2026-06-30	4.3	CVE-2026-58373
DALIBO-- PostgreSQL Anonymizer	PostgreSQL Anonymizer contains a vulnerability that allows unprivileged masked users to repeatedly call the anon.hash() function and collects (seed, hash_output) pairs to perform an offline brute-force attack and deduce the salt. The problem is resolved in PostgreSQL Anonymizer 3.1.2 and later versions	2026-06-30	4.3	CVE-2026-13455
DeepMyst--Mysti	A weakness has been identified in DeepMyst Mysti 0.4.0. Affected is the function _isTrackedConversation of the file src/managers/ChannelBridge.ts of the component Contact Tracking. This manipulation of the argument _channelType causes improper authorization. The attack may be initiated remotely. A high degree of complexity is needed for the attack. The exploitability is told to be difficult. The exploit has been made available to the public and could be used for attacks. Patch name:	2026-06-29	5	CVE-2026-13591

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	9b4aff0f106db424aa45a35aa89dd0b8f2eb9a48. It is suggested to install a patch to address this issue.			
DeepMyst--Mysti	A vulnerability has been found in DeepMyst Mysti up to 0.4.0. The affected element is the function initProjectMemory of the file src/managers/MemoryManager.ts of the component Per-Project Auto-Memory Handler. Such manipulation of the argument workspacePath leads to exposure of resource. The attack may be performed from remote. Upgrading to version 0.4.0 is sufficient to fix this issue. The name of the patch is 6d709229b5199f6769fb3cf763e5122dcc43c079. It is advisable to upgrade the affected component.	2026-07-03	4.3	CVE-2026-14611
Dell--Inspiron 15 3520	Dell Client Platform BIOS contains an Authentication Bypass by Primary Weakness vulnerability. An unauthenticated attacker with physical access could potentially exploit this vulnerability, leading to Information Disclosure.	2026-07-03	5.3	CVE-2026-35159
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper neutralization of special Elements used in an OS command ('OS command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to command execution.	2026-07-03	6.5	CVE-2026-26355
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an integer overflow or wraparound vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to denial of service.	2026-07-03	6.5	CVE-2026-46463
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper neutralization of special elements used in an OS command ('OS command Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution.	2026-07-03	6.7	CVE-2026-49813
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper neutralization of special elements used in an OS command ('OS command Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution.	2026-07-03	6.7	CVE-2026-54483
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an use of externally-controlled format string vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure and denial of service.	2026-07-03	5.5	CVE-2026-46465

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an insertion of sensitive information into log file vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to information exposure.	2026-07-03	5.8	CVE-2026-46467
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper access control vulnerability in the RBAC. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to information tampering.	2026-07-03	4.3	CVE-2026-41123
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an incorrect permission Assignment for critical resource vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to unauthorized access.	2026-07-03	4.4	CVE-2026-44268
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper link resolution before file access ('link following') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to unauthorized access.	2026-07-03	4.4	CVE-2026-44269
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper link resolution before file access ('Link following') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to information disclosure.	2026-07-03	4.9	CVE-2026-46464
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an improper link resolution before file access ('Link following') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to information exposure.	2026-07-03	4.4	CVE-2026-46468
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an incorrect authorization vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to unauthorized command execution.	2026-07-03	4.2	CVE-2026-46730
DivvyDrive Information Technologies Inc.--DivvyDrive	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in DivvyDrive Information Technologies Inc. DivvyDrive allows Stored XSS. This issue affects DivvyDrive: from 4.8.2.23 before v.4.8.3.1.	2026-07-01	6.4	CVE-2026-5220

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
DivvyDrive Information Technologies Inc.--DivvyDrive	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in DivvyDrive Information Technologies Inc. DivvyDrive allows Stored XSS. This issue affects DivvyDrive: from v.4.8.2.23 before v.4.8.3.1.	2026-07-01	5.4	CVE-2026-6283
Documenso--Documenso	A vulnerability was detected in Documenso up to 2.11.0. Affected by this vulnerability is an unknown functionality of the file packages/auth/server/lib/utls/handle-oauth-callback-url.ts of the component Google OAuth Login. The manipulation results in improper authentication. It is possible to launch the attack remotely. This attack is characterized by high complexity. The exploitation appears to be difficult. The exploit is now public and may be used. The pull request to fix this issue awaits acceptance.	2026-06-29	5.6	CVE-2026-13543
drfuri--Martfury - WooCommerce Marketplace WordPress Theme	Subscriber Broken Access Control in Martfury - WooCommerce Marketplace WordPress Theme <= 3.2.8 versions.	2026-07-02	4.3	CVE-2026-57685
dromara--RuoYi-Vue-Plus	RuoYi-Vue-Plus through 5.6.2, fixed in commit 88d03d9, exposes workflow task management endpoints under /workflow/task (FlwTaskController) without any permission check: the controller declares no class-level or method-level authorization annotation, so the endpoints are gated only by global authentication. Any authenticated user, regardless of assigned role, can therefore reassign workflow approval tasks to arbitrary users via updateAssignee (defeating segregation of duties in the approval process), urge arbitrary tasks, and enumerate all pending and finished tasks via the pageByAllTaskWait and pageByAllTaskFinish listing endpoints. The issue was resolved by adding permission identifiers (SaCheckPermission) to these endpoints.	2026-06-30	6.5	CVE-2026-58176
dylan ngo--Woostify Sites Library	Unauthenticated Broken Access Control in Woostify Sites Library <= 1.6.2 versions.	2026-07-02	5.3	CVE-2025-66076
e4jvikwp--VikBooking Hotel Booking Engine & PMS	The VikBooking Hotel Booking Engine & PMS plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'layoutstyle' parameter in all versions up to, and including, 1.8.12 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. Exploitation requires the targeted page to render the [vikbooking view="roomslist"] shortcode, as the vulnerable layoutstyle parameter is only processed in that view context.	2026-07-01	6.1	CVE-2026-12754
Eclipse Foundation--Eclipse Open VSX	In Open VSX Registry before 1.0.2, the /vscode/unpkg/ endpoint serves user-supplied HTML files with Content-Type: text/html and without a Content-Security-Policy or Content-Disposition: attachment response header. An unauthenticated attacker can register a publisher account, upload a VSIX containing a crafted HTML payload, and induce an authenticated user to visit the resulting URL. The browser renders the file inline in the open-vsx.org origin context, enabling session token exfiltration, persistent Personal Access Token (PAT) generation, and unauthorized publication of malicious extension versions. Because Open	2026-07-01	4.1	CVE-2026-13323

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	VSX extensions are distributed to VS Code, VSCodeium, Cursor, Windsurf, and compatible editors, a compromised extension update constitutes a supply chain attack against all downstream users.			
edge22--GenerateBlocks	The GenerateBlocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Headline Block 'linkMetaFieldType' Dynamic Link Attribute in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. A contributor-level attacker can store a JavaScript payload in their own profile description (allowlisted by get_safe_user_meta_keys()) and prepend 'javascript:' via the linkMetaFieldType attribute, creating a fully attacker-controlled href that executes when any user, including an administrator, clicks the rendered headline link.	2026-07-03	6.4	CVE-2026-9756
Edimax--EW-7478APC	A security vulnerability has been detected in Edimax EW-7478APC 1.04. The affected element is the function formAccept of the file /goform/formAccept of the component POST Request Handler. The manipulation of the argument submit-url leads to os command injection. The attack is possible to be carried out remotely. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-29	6.3	CVE-2026-13560
Edimax--EW-7478APC	A vulnerability was detected in Edimax EW-7478APC 1.04. The impacted element is the function formiNICbasic of the file /goform/formiNICbasic of the component POST Request Handler. The manipulation of the argument rootAPmac results in os command injection. The attack may be performed from remote. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-29	6.3	CVE-2026-13561
Edimax--EW-7478APC	A vulnerability was detected in Edimax EW-7478APC 1.04. This vulnerability affects the function formStaDrvSetup of the file /goform/formStaDrvSetup of the component POST Request Handler. The manipulation of the argument rootAPmac results in os command injection. The attack can be executed remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-29	6.3	CVE-2026-13581
Eksagate Electronic Engineering and Computer Industry Trade Inc.--SYSGUARD 6001	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Eksagate Electronic Engineering and Computer Industry Trade Inc. SYSGUARD 6001 allows Stored XSS. This issue affects SYSGUARD 6001: from 2.0.2 before 6.1.4.0. NOTE: The vendor was contacted and it was learned that the product is not supported.	2026-06-30	6.1	CVE-2026-8403
Elastic--Elastic Defend	Incorrect Authorization (CWE-863) in Elastic Defend can lead to unauthorized information disclosure via Accessing Functionality Not Properly Constrained by ACLs (CAPEC-1). Under certain conditions, a low-privileged authenticated user can access response action data that they are not authorized to view.	2026-07-01	5.3	CVE-2026-56152
Elastic--Elasticsearch	Uncontrolled Resource Consumption (CWE-400) in Elasticsearch can lead to a denial of service via Excessive Allocation (CAPEC-130). An authenticated user can submit a specially crafted bulk request that causes	2026-07-01	6.5	CVE-2026-49090

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sustained high CPU consumption, which can render the affected node unable to process requests.			
Elastic--Elasticsearch	Uncontrolled Recursion (CWE-674) in Elasticsearch can lead to a denial of service via Excessive Allocation (CAPEC-130). An authenticated user can submit a specially crafted query that causes excessive resource consumption while the request is processed, which may render the affected node unavailable.	2026-07-01	6.5	CVE-2026-56148
Elastic--Elasticsearch	Allocation of Resources Without Limits or Throttling (CWE-770) in Elasticsearch can lead to a denial of service via Excessive Allocation (CAPEC-130). A user with elevated privileges can submit a specially crafted machine learning request that causes excessive memory consumption, which may render the affected node unavailable.	2026-07-01	4.9	CVE-2026-56149
Elastic--Fleet Server	Allocation of Resources Without Limits or Throttling (CWE-770) in Fleet Server can lead to a denial of service via Excessive Allocation (CAPEC-130). An attacker can submit a specially crafted request to an upload endpoint that causes excessive memory consumption, which may render Fleet Server unavailable.	2026-07-01	6.5	CVE-2026-56150
Elastic--Kibana	Allocation of Resources Without Limits or Throttling (CWE-770) in Kibana can lead to a denial of service via Excessive Allocation (CAPEC-130). An authenticated user can submit a specially crafted bulk deletion request that causes excessive resource consumption, which may render Kibana unavailable.	2026-07-01	6.5	CVE-2026-49087
Elastic--Kibana	Improper Input Validation (CWE-20) in Kibana can lead to a denial of service via Input Data Manipulation (CAPEC-153). An authenticated user can submit a specially crafted Fleet policy input that is not correctly validated, which can render Fleet agent, server, and policy management functionality unavailable.	2026-07-01	6.5	CVE-2026-56151
Elastic--Kibana	Insertion of Sensitive Information into Log File (CWE-532) in Kibana can lead to information disclosure. When the optional application performance monitoring (APM) instrumentation is enabled, sensitive request header values could be recorded in application logs, where they may be accessible to operators with log access.	2026-07-01	4.4	CVE-2026-49088
engagementanalytics--Plugin for Google Analytics by IO technologies	The Plugin for Google Analytics by IO technologies plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.1. This is due to missing or incorrect nonce validation on the Google Analytics settings page (ga.php). This makes it possible for unauthenticated attackers to update the plugin's stored Google Analytics tracking ID option (io-ga-id) via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-06-30	4.3	CVE-2026-8944
envothemes--Envo's Templates & Widgets for Elementor and WooCommerce	The Envo's Templates & Widgets for Elementor and WooCommerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing authorization check on the Envo Tabs (and Off Canvas) widget's template rendering in versions up to, and including, 1.4.26. The render() method of the Tabs widget passes a user-controlled template/post ID directly to Elementor's get_builder_content_for_display() without verifying the referenced post's status (published/private/draft) or the visitor's authorization to view it. This makes it possible for authenticated attackers, with Author-level access and above, to disclose the contents of	2026-07-02	4.3	CVE-2026-11600

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	private Elementor-driven pages and templates to anonymous visitors by configuring an Envo Tabs widget on a public post to reference the private content's ID (which can be supplied by editing the underlying Elementor widget JSON via the Elementor editor REST API).			
EstrellaXD--Auto_Bangumi	AutoBangumi before 3.2.8 contains a server-side request forgery (SSRF) vulnerability that allows unauthenticated remote attackers to probe internal network services by supplying arbitrary host values to an unprotected setup endpoint. Attackers can send requests to the POST /api/v1/setup/test-downloader endpoint during the initial setup window, causing the server to issue HTTP GET requests to internal or reserved addresses and leak information through echoed connection-error messages.	2026-07-02	5.8	CVE-2026-59101
expresstech--Quiz and Survey Master (QSM) Easy Quiz and Survey Maker	The Quiz and Survey Master (QSM) - Easy Quiz and Survey Maker plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 11.1.4. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to modify quizzes they do not own, overwrite quiz results pages, and reroute quiz-result notification emails to attacker-controlled addresses. An attacker first calls the /quiz/structure endpoint with an arbitrary victim quiz ID to obtain a valid nonce bound to that quiz ID and their own user ID, then presents that nonce to the /quizzes/{id}/emails/save endpoint, which accepts it without verifying quiz ownership.	2026-07-03	4.3	CVE-2026-9230
Feehi--CMS	A flaw has been found in Feehi CMS up to 2.1.1. Affected by this issue is some unknown functionality of the file /api/users of the component API. This manipulation causes improper access controls. The attack can be initiated remotely. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-29	6.3	CVE-2026-13544
figureone--Insert Pages	The Insert Pages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via post custom field keys (meta key names) in all versions up to, and including, 3.11.4. This is due to insufficient output escaping in the the_meta() function: while the custom field VALUE is sanitized with wp_kses_post(), the custom field KEY (\$key) is interpolated into the rendered HTML (lines 1786-1791) and echoed (line 1806) without any escaping when an inserted page is rendered with the [insert page='ID' display='all'] shortcode. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-02	6.4	CVE-2026-10089
foliovision--FV Flowplayer Video Player	The FV Flowplayer Video Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'video_player' shortcode 'align' attribute in all versions up to, and including, 7.5.51.7212 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-01	6.4	CVE-2026-12135
forgejo--forgejo	Forgejo before 15.0.3 contains a stored cross-site scripting vulnerability that allows authenticated attackers to execute arbitrary JavaScript in other users' browsers by setting a full name containing an HTML payload and	2026-07-02	5.4	CVE-2026-59102

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	triggering an Actions run. When the DEFAULT_SHOW_FULL_NAME option is enabled, the run description is assembled server-side with the user's display name interpolated into an HTML string via a translation function that does not escape its arguments, and the frontend renders the result using a Vue v-html binding, causing script execution for any user who views the affected Actions run page.			
Fuelthemes--Werkstatt	Subscriber Broken Access Control in Werkstatt <= 4.7.2 versions.	2026-07-02	4.3	CVE-2026-57689
Fuelthemes--Werkstatt	Unauthenticated Cross Site Request Forgery (CSRF) in Werkstatt <= 4.7.2 versions.	2026-07-02	4.3	CVE-2026-57690
Gardyn--Gardyn Home Firmware	The admin panel lacks standard security headers, enabling clickjacking and cross-site scripting attacks.	2026-07-02	5.4	CVE-2026-54477
Gardyn--Gardyn Home Firmware	The Azure Blob Storage container used for Gardyn device logs is publicly listable without authentication. A malicious user would be able to access any device log file available in the blob storage container.	2026-07-02	5.3	CVE-2026-55726
genua--genucenter	The genucenter web interface before version 8.0p11 unnecessarily exposes sensitive SNMP authentication and encryption keys in its HTTP responses to users with the "Service" or "Admin" role.	2026-07-01	4.3	CVE-2026-13211
GitBucket--GitBucket	A security flaw has been discovered in GitBucket up to 4.46.1. This affects the function Git.cloneRepository.setURI of the file src/main/scala/gitbucket/core/service/RepositoryCreationService.scala. Performing a manipulation of the argument url results in server-side request forgery. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The patch is named 487a9b980f56aa73b6a044b1e86a92eed5043215. To fix this issue, it is recommended to deploy a patch.	2026-06-29	6.3	CVE-2026-13540
Gitea--Gitea Open Source Git Server	SSRF via HTTP Redirect in Repository Migration	2026-07-03	6.5	CVE-2026-58418
Gitea--Gitea Open Source Git Server	Gitea versions up to and including 1.26.1 do not apply public-only token filtering consistently to the user organization API, leaving an incomplete fix for CVE-2025-68941.	2026-07-03	4.3	CVE-2026-25714
Gitea--Gitea Open Source Git Server	Gitea versions up to and including 1.26.2 allow repository RSS and Atom feed endpoints to bypass API access token scope checks, exposing private repository commit data to tokens without the required repository scope.	2026-07-03	4.3	CVE-2026-27761
Gitea--Gitea Open Source Git Server	Gitea versions up to and including 1.26.1 do not enforce repository-unit authorization on issue-template API endpoints.	2026-07-03	4.3	CVE-2026-27783
GNOME--GLib	A flaw was found in GLib. An off-by-one error can occur in the gvs_tuple_is_normal function in the glib/gvariant-serialiser.c file when doing an alignment padding check because the bounds check uses > instead of >=, causing an out-of-bounds read of only 1 byte. This issue can cause a minor information disclosure of 1 byte and a denial of service when the out-of-bounds read crosses a page boundary.	2026-06-30	6.5	CVE-2026-58010

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
GNOME--GLib	A flaw was found in GLib. An out-of-bounds read of only 2 bytes can occur in the <code>g_date_time_get_ymd</code> function in the <code>glib/gdatetime.c</code> file when an invalid <code>GDateTime</code> object produced by the <code>g_date_time_add_full</code> function is processed. This flaw can corrupt the date output and potentially cause logic errors that may lead to a denial of service.	2026-06-30	6.5	CVE-2026-58011
GNOME--GLib	A flaw was found in GLib. A buffer over-read can occur in the <code>g_regex_replace</code> function when used with the <code>'G_REGEX_RAW'</code> compile flag and case-change replacement escapes because the <code>string_append</code> function processes matched substrings using UTF-8 functions that assume valid UTF-8 input, even when the string is treated as raw bytes. This vulnerability can cause a minor information disclosure of 1-5 bytes and a denial of service when the buffer over-read crosses a page boundary.	2026-06-30	6.5	CVE-2026-58012
GNOME--GLib	A flaw was found in GLib. A buffer over-read can occur in <code>g_io_channel_read_line_backend()</code> in the <code>giochannel.c</code> file when a custom line terminator with a length greater than one is set, causing <code>memcmp</code> to read past the <code>GString</code> buffer. This vulnerability can cause a minor information disclosure of 7 bytes or a denial of service when the buffer over-read crosses a page boundary.	2026-06-30	6.5	CVE-2026-58013
GNOME--GLib	A flaw was found in GLib. The D-Bus client-side implementation of the <code>DBUS_COOKIE_SHA1</code> SASL authentication mechanism does not validate the <code>cookie_context</code> parameter received from the server. A malicious D-Bus server can supply a <code>cookie_context</code> containing path traversal sequences, causing the client to read an arbitrary file and exfiltrate sensitive data by verifying guessed file contents against a generated hash.	2026-06-30	5.9	CVE-2026-58015
Gordon Bhme--Structured Content	Contributor Cross Site Scripting (XSS) in Structured Content <= 1.7.0 versions.	2026-07-02	6.5	CVE-2026-57763
GotoHTTP--GotoHTTP	A vulnerability has been found in GotoHTTP up to 10.2. This issue affects some unknown processing of the file <code>/reg.12x</code> . The manipulation of the argument <code>sn</code> leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor explains: "We immediately removed unnecessary parameter <code>echo</code> from source code. However the URL in the issue description will never be used in browser nor exposed to user, so it will not bring secure problem in fact. So we don't upgrade server right now, it will be included in next version together with other features."	2026-06-29	4.3	CVE-2026-13536
guardian--language-system	Guardian language-system fails to sanitize the name GET parameter before outputting it into an HTML input value attribute in <code>designer.php</code> (line 57). An authenticated attacker can craft a URL containing script tags that execute in the victim's browser session.	2026-07-01	4.6	CVE-2026-34096
guardian--language-system	Guardian language-system fails to sanitize the id GET parameter before inserting it into multiple HTML form action attributes in <code>text_file.php</code> (lines 94, 101, 323, 403, 826, 852). An authenticated attacker can craft a URL that injects script tags executing in the victim's browser session.	2026-07-01	4.6	CVE-2026-34097
guardian--language-system	Guardian language-system fails to sanitize the id GET parameter before inserting it into HTML source and form action attributes in <code>media.php</code>	2026-07-01	4.6	CVE-2026-34098

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(lines 119, 129). An authenticated attacker can craft a URL that injects script tags executing in the victim's browser session.			
HashiCorp--Vault	HashiCorp Vault and Vault Enterprise prior to 2.0.1 audit device validation logic did not consistently apply plugin directory protections when the legacy file audit path option was used. This vulnerability (CVE-2026-5051) is fixed in 2.0.1, 1.21.6, 1.20.11, and 1.19.17.	2026-07-01	4.4	CVE-2026-5051
HCLSoftware--HCL DevOps Deploy / HCL Launch	HCL DevOps Deploy / HCL Launch is susceptible to an exposure of sensitive information vulnerability in output logs. This exposure could allow an attacker with access to the logs to potentially obtain sensitive values related to that step.	2026-06-29	4.3	CVE-2026-56457
HiEventsDev--Hi.Events	Hi.Events through 1.9.0 public check-in list endpoints use short_id as sole access control, allowing unauthenticated access to retrieve full attendee lists including emails and personal information. Attackers with knowledge of the short_id can call GET /api/public/check-in-lists/{short_id}/attendees to read attendee data and create or delete check-in records without authentication.	2026-06-29	6.5	CVE-2026-57960
HiEventsDev--Hi.Events	Hi.Events through 1.9.0 contains a promo code validation vulnerability where reservation validates usage count before asynchronous UpdateEventStatisticsJob increments it, allowing attackers to redeem limited promo codes unlimited times. Attackers can sequentially reserve multiple orders with the same restricted promo code, each reading order_usage_count=0 and passing validation, then complete them all at discounted prices without concurrent requests.	2026-06-29	5.9	CVE-2026-57959
Hitachi--Hitachi Virtual Storage Platform 5100, 5200, 5500, 5600, 5100H, 5200H, 5500H, 5600H, VX8	Information exposure vulnerability in Hitachi Storage Navigator. This issue affects Hitachi Virtual Storage Platform 5100, 5200, 5500, 5600, 5100H, 5200H, 5500H, 5600H, VX8: before DKCMAIN Ver. 90-09-24-00/00, SVP Ver. 90-09-24/00, before DKCMAIN Ver. 90-08-86-00/00, SVP Ver. 90-08-86/00; Hitachi Virtual Storage Platform G1000, G1500, F1500, VX7: before DKCMAIN Ver. 80-06-96-00/00, SVP Ver. 80-06-91/00.	2026-06-29	6.8	CVE-2025-7386
HKUDS--Vibe-Trading	Vibe-Trading before 0.1.10 contains a path traversal vulnerability that allows attackers to write files outside the intended memory root directory by supplying a malicious memory_type value containing path traversal sequences through the remember tool. Attackers can manipulate the memory_type parameter in the persistent memory store to cause the application to write arbitrary Markdown files to unintended locations on the filesystem.	2026-06-30	6.5	CVE-2026-58173
HKUDS--Vibe-Trading	Vibe-Trading before 0.1.10 constructs the swarm run directory by joining a caller-supplied run identifier onto the runs base directory without validation in run_dir (agent/src/swarm/store.py). A crafted run identifier supplied through the MCP swarm tools causes the application to read arbitrary run.json files outside the runs directory and to overwrite existing run.json files at traversed locations.	2026-06-30	4.2	CVE-2026-58171
Hono--Hono	Hono before 4.10.2 (fixed in 4.10.3) contains a flaw in its CORS middleware: when the origin is not set to "*", the middleware copies the Vary header from the incoming request into the response. Because Vary is a response header that should be managed by the server, an attacker can supply arbitrary Vary values that are reflected into the response,	2026-06-30	6.5	CVE-2025-71381

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	potentially causing cache key pollution and inconsistent CORS enforcement in environments that rely on shared caches or proxies.			
horde--imp	Horde IMP before 7.0.1 contains a path traversal vulnerability in lib/Compose.php that allows authenticated attackers to read arbitrary files from the server filesystem by embedding traversal sequences after a CKEditor path prefix in img src URLs. Attackers can bypass the stripos() prefix validation by appending sequences such as traversal segments after the matching prefix, causing file_get_contents() to read sensitive files whose contents are then exfiltrated as MIME parts in outgoing email; unauthenticated exploitation is also achievable via CSRF against an active authenticated session.	2026-07-01	6.5	CVE-2026-58451
IBM--App Connect Enterprise	IBM App Connect Enterprise 13.0.1.0 through 13.0.7.2, and 12.0.1.0 through 12.0.12.26 and IBM Integration Bus for z/OS 10.1.0.0 through 10.1.0.7 is vulnerable to SQL injection. A remote attacker could socially engineer a user into accidentally creating files they may not be aware of.	2026-06-30	4.7	CVE-2026-3602
IBM--Db2	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 for Linux, UNIX and Windows (includes Db2 Connect Server) could allow an authenticated user to cause a denial of service due to improper neutralization of special elements in the data query logic of XMLTable-derived columns.	2026-06-30	6.5	CVE-2026-11906
IBM--Db2	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 for Linux, UNIX and Windows (includes Db2 Connect Server) could disclose sensitive information to an authenticated user from the monitoring and event tables.	2026-06-30	5.5	CVE-2025-36372
IBM--UCD - IBM DevOps Deploy	IBM UCD - IBM DevOps Deploy 8.1 through 8.1.2.6, and 8.2 through 8.2.1.0 uses Cross-Origin Resource Sharing (CORS) which could allow an attacker to carry out privileged actions and retrieve sensitive information as the domain name is not being limited to only trusted domains.	2026-06-30	5.4	CVE-2026-12084
IBM--UCD - IBM UrbanCode Deploy	IBM UCD - IBM UrbanCode Deploy 7.3 through 7.3.2.18 and IBM UCD - IBM DevOps Deploy 8.0 through 8.0.1.13, 8.1 through 8.1.2.6, and 8.2 through 8.2.1.0 IBM DevOps Deploy could disclose sensitive configurations and secrets to authenticated users in API responses that could be used in further attacks against the system.	2026-06-30	6.5	CVE-2026-12085
IBM--UCD - IBM UrbanCode Deploy	IBM UCD - IBM UrbanCode Deploy 7.2 through 7.2.3.23, and 7.3 through 7.3.2.18 and IBM UCD - IBM DevOps Deploy 8.0 through 8.0.1.13, 8.1 through 8.1.2.6, and 8.2 through 8.2.1.0 stores potentially sensitive information in log files that could be read by a local user.	2026-06-30	6.2	CVE-2026-12086
IBM--watsonx.data intelligence	IBM watsonx.data intelligence 5.2.0, 5.2.1, 5.2.2, 5.3.0 is vulnerable to stored cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-06-30	6.4	CVE-2025-36320
IBM--watsonx.data intelligence	IBM watsonx.data intelligence 5.2.0, 5.2.1, 5.2.2, 5.3.0 could allow an authenticated user to bypass security controls and perform unauthorized actions due to client-side enforcement of sever-side security.	2026-06-30	6.5	CVE-2025-36327

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
IBM--watsonx.data intelligence	IBM watsonx.data intelligence 5.2.2, 5.3.0, 5.3.1, 5.3.1 through patch-1 transmits data in clear text that could allow an attacker to obtain sensitive information using man in the middle techniques.	2026-06-30	5.9	CVE-2025-12530
IBM--watsonx.data intelligence	IBM watsonx.data intelligence 5.2.0, 5.2.1, 5.2.2, 5.3.0 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site.	2026-06-30	5.7	CVE-2025-36321
IBM--watsonx.data intelligence	IBM watsonx.data intelligence 5.2.0, 5.2.1, 5.2.2, 5.3.0 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-06-30	5.4	CVE-2025-36323
IBM--watsonx.data intelligence	IBM watsonx.data intelligence 5.2.0, 5.2.1, 5.2.2, 5.3.0 transmits data in clear text that could allow an attacker to obtain sensitive information using man in the middle techniques.	2026-06-30	5.9	CVE-2025-36336
IBM--watsonx.data intelligence	IBM watsonx.data intelligence 5.2.0, 5.2.1, 5.2.2, 5.3.0 could allow an authenticated user to cause a temporary denial using a specially crafted HTTP request due to improper allocation of resource throttling.	2026-06-30	4.3	CVE-2025-36319
IBM--watsonx.data intelligence	IBM watsonx.data intelligence 5.2.0, 5.2.1, 5.2.2, 5.3.0 s vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks.	2026-06-30	4.3	CVE-2025-36324
IBM--watsonx.data intelligence	IBM watsonx.data intelligence 5.2.0, 5.2.1, 5.2.2, 5.3.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.	2026-06-30	4.3	CVE-2025-36328
IBM--watsonx.data intelligence	IBM watsonx.data intelligence 5.2.0, 5.2.1, 5.2.2, 5.3.0 could allow an authenticated user to perform unauthorized actions due to the improper enforcement of behavioral workflow.	2026-06-30	4.3	CVE-2025-36333
IBM--WebSphere Application Server	IBM WebSphere Application Server 9.0, and 8.5 could allow a remote attacker to obtain sensitive information from the administrative console's integrated help system.	2026-06-30	4.3	CVE-2026-11595
IBM--WebSphere Extreme Scale	IBM WebSphere Extreme Scale 8.6.1.0 through 8.6.1.6 Approximately 50 generated CORBA stub classes in WebSphere eXtreme Scale's ogclient.jar call ORB.string_to_object() on an attacker-controlled IOR string during Java deserialization, turning any unfiltered ObjectInputStream sink in WAS into outbound IIOP SSRF to an attacker-chosen host; when chained with the IBM ORB's getUserException class-instantiation flaw (WAS-26), this SSRF escalates to remote code execution on the calling JVM.	2026-06-30	6	CVE-2026-13773
IBM--WebSphere Extreme Scale	IBM WebSphere Extreme Scale 8.6.1.0 through 8.6.1.6 could allow an adjacent attacker to cause a denial of service due to improper validation in the XDF decoder. The application processes deeply nested Protocol Buffers messages and attacker-controlled length prefixes without sufficient bounds checking, which may allow an attacker on the same network to trigger a StackOverflowError or OutOfMemoryError, resulting in a crash of the WebSphere Application Server JVM.	2026-06-30	6.5	CVE-2026-9002

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
icegram--Email Subscribers & Newsletters Email Marketing, Post Notifications & Newsletter Plugin for WordPress	The Email Subscribers & Newsletters - Email Marketing, Post Notifications & Newsletter Plugin for WordPress plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.9.27. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to overwrite plugin mail settings (from name and from email address), create audience lists, insert arbitrary contacts into those lists, create and overwrite newsletter broadcasts and post notifications, add workflows, and queue and dispatch mass email to arbitrary recipients.	2026-07-02	4.3	CVE-2026-11592
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-51 and 7.1.2-26, an integer overflow in the XCF decoder can result in an out of bounds read when a crafted image is read, potentially resulting in a crash. This issue has been fixed in versions 6.9.13-51 and 7.1.2-26.	2026-07-01	6.5	CVE-2026-53466
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-51 and 7.1.2-26, the MNG decoder contains a possible heap information disclosure vulnerability because part of the pixels are left unchanged. This issue has been fixed in versions 6.9.13-51 and 7.1.2-26.	2026-07-01	5.3	CVE-2026-53467
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-51 and 7.1.2-26, when identifying an image with a crafted 8BIM profile with a specific format string a use-after-free will occur. This issue has been fixed in versions 6.9.13-51 and 7.1.2-26.	2026-07-01	5.5	CVE-2026-55510
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-51 and 7.1.2-26, a heap buffer overflow occurs in the MVG decoder that could result in an out of bounds write when processing a crafted image. This issue has been fixed in versions 6.9.13-51 and 7.1.2-26.	2026-07-01	5.9	CVE-2026-55577
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-51 and 7.1.2-26, a missing depth check in the MVG decoder will result in a stack overflow when a crafted image is provided. This issue has been fixed in versions 6.9.13-51 and 7.1.2-26.	2026-07-01	5.3	CVE-2026-55594
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to version 7.1.2-26, an incorrect handling of arguments can cause a heap buffer over-write in the JP2 encoder. This issue has been fixed in version 7.1.2-26.	2026-07-01	5.5	CVE-2026-55597
ImageMagick--ImageMagick	In versions prior to 7.1.2-26, the `concatenate` operation is missing policy checks, potentially resulting in both reading and writing to paths disallowed by the security policy. This issue has been fixed in version 7.1.2-26.	2026-07-01	5.5	CVE-2026-55628
ImageMagick--ImageMagick	ImageMagick is free and open-source software used for editing and manipulating digital images. Prior to versions 6.9.13-51 and 7.1.2-26, when providing invalid arguments to the connected-components option an	2026-07-01	4.7	CVE-2026-55595

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	infinite loop will occur. This issue has been fixed in versions 6.9.13-51 and 7.1.2-26.			
infiniflow--ragflow	RAGFlow before 0.26.3 stores an agent pipeline (DSL) node name without sanitization: the agent update endpoint normalizes the submitted DSL via <code>normalize_dsl</code> , which only performs JSON serialization validation and preserves the node name verbatim. The dataflow-result web UI then renders that name into the "Rerun from current step" confirmation modal via <code>dangerouslySetInnerHTML</code> , and the <code>next</code> configuration sets <code>escapeValue:false</code> , so the value is inserted into the DOM without HTML encoding. An authenticated workspace user who can create or edit an agent can inject arbitrary JavaScript that executes in the session of another workspace member who opens the dataflow result and clicks rerun, enabling session/token theft and account takeover across the user trust boundary.	2026-07-02	5.4	CVE-2026-58579
inovector--mixpost	Mixpost through 2.6.0 contains a reflected cross-site scripting vulnerability that allows unauthenticated attackers to execute arbitrary JavaScript in authenticated users' browsers by crafting malicious OAuth callback URLs with unsanitized error query parameters. Attackers can exploit the OAuth callback controller's failure to sanitize error parameters before rendering them through Laravel flash messages via the Vue <code>v-html</code> directive to hijack authenticated user sessions or perform unauthorized actions.	2026-06-29	6.1	CVE-2026-57958
Investintech--SlimPDFReader	A security flaw has been discovered in Investintech SlimPDFReader up to 2.0.14. Affected by this issue is the function <code>SlimPDFReader!Investintech::PCV::TeighaDo+0x25cde0</code> of the file <code>SlimPDFReader.exe</code> of the component PDF File Handler. Performing a manipulation results in out-of-bounds read. It is possible to initiate the attack remotely. This vulnerability only affects products that are no longer supported by the maintainer.	2026-06-29	4.3	CVE-2026-13522
invoiceninja--invoiceninja	Invoice Ninja through 5.13.26 contains an open redirect vulnerability in the client portal login that allows unauthenticated attackers to redirect authenticated victims to attacker-controlled external URLs by injecting a malicious value into the intended query parameter. Attackers can craft a client login link with an external URL in the intended parameter, which is stored in the session without host validation and emitted verbatim via a bare redirect in the <code>ContactLoginController authenticated()</code> handler after the victim completes a legitimate login, enabling phishing attacks.	2026-06-30	4.3	CVE-2026-58450
its-a-feature--Mythic	Mythic before 3.4.0.60 contains a broken hasura permission filter on the <code>payload_build_step</code> table with an always-satisfied <code>_or</code> condition that bypasses operation-scoped access controls. Authenticated operators and spectators can query <code>payload_build_step</code> to read <code>step_stdout</code> , <code>step_stderr</code> , <code>step_name</code> , and <code>step_description</code> across all operations on the server.	2026-06-29	6.5	CVE-2026-57951
its-a-feature--Mythic	Mythic before 3.4.0.60 contains an authorization bypass vulnerability in four REST endpoints (<code>c2profile_config_check_webhook</code> , <code>c2profile_redirect_rules_webhook</code> , <code>c2profile_get_ioc_webhook</code> , <code>c2profile_sample_message_webhook</code>) that fail to verify payload ownership. An operator in one operation can invoke these endpoints with a known payload UUID from another operation to access that operation's C2 profile configuration including encryption keys and callback parameters.	2026-06-29	5.3	CVE-2026-57952

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
its-a-feature--Mythic	Mythic before 3.4.0.60 contains an authorization bypass vulnerability that allows authenticated spectator-role users to perform unauthorized write operations by accessing the eventing_import_automatic_webhook endpoint registered under spectator-permitted middleware. Attackers with spectator role can exploit this misconfigured access control to create and delete automation workflows, making unauthorized modifications to operation automation configuration and EventGroups.	2026-06-29	5.4	CVE-2026-57953
itsourcecode--Hospital Management System	A vulnerability was determined in itsourcecode Hospital Management System 1.0. Affected is an unknown function of the file /appointmentapproval.php of the component Appointment Handler. This manipulation of the argument editid causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.	2026-06-29	6.3	CVE-2026-13520
itsourcecode--Hospital Management System	A vulnerability was identified in itsourcecode Hospital Management System 1.0. This impacts an unknown function of the file /appointmentdetail.php of the component Appointment Handler. The manipulation of the argument editid leads to sql injection. The attack is possible to be carried out remotely. The exploit is publicly available and might be used.	2026-06-29	6.3	CVE-2026-13530
itsourcecode--Hospital Management System	A security flaw has been discovered in itsourcecode Hospital Management System 1.0. Affected is an unknown function of the file /department.php. The manipulation of the argument editid results in sql injection. The attack may be performed from remote. The exploit has been released to the public and may be used for attacks.	2026-06-29	6.3	CVE-2026-13531
itsourcecode--Hospital Management System	A weakness has been identified in itsourcecode Hospital Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /departmentDoctor.php. This manipulation of the argument deptid causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks.	2026-06-29	6.3	CVE-2026-13532
itsourcecode--Hospital Management System	A weakness has been identified in itsourcecode Hospital Management System 1.0. This impacts an unknown function of the file /doctorchangepassword.php. Executing a manipulation of the argument newpassword can lead to sql injection. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	2026-06-29	6.3	CVE-2026-13541
itsourcecode--Hospital Management System	A security vulnerability has been detected in itsourcecode Hospital Management System 1.0. Affected is an unknown function of the file /doctorprofile.php. The manipulation of the argument doctorname leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	2026-06-29	6.3	CVE-2026-13542
itsourcecode--Hospital Management System	A vulnerability was identified in itsourcecode Hospital Management System 1.0. Impacted is an unknown function of the file /doctortimings.php. The manipulation of the argument editid leads to sql injection. Remote exploitation of the attack is possible. The exploit is publicly available and might be used.	2026-06-29	6.3	CVE-2026-13548

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
itsourcecode--Hospital Management System	A vulnerability has been found in itsourcecode Hospital Management System 1.0. The impacted element is an unknown function of the file /insertbillingrecord.php. The manipulation of the argument patientid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2026-06-29	6.3	CVE-2026-13572
itsourcecode--Hospital Management System	A security flaw has been discovered in itsourcecode Hospital Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /patientdetail.php. Performing a manipulation of the argument editid results in sql injection. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	2026-06-29	6.3	CVE-2026-13578
itsourcecode--Hospital Management System	A weakness has been identified in itsourcecode Hospital Management System 1.0. Affected by this issue is some unknown functionality of the file /patientchangepassword.php. Executing a manipulation of the argument newpassword can lead to sql injection. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks.	2026-06-29	6.3	CVE-2026-13579
itsourcecode--Hospital Management System	A flaw has been found in itsourcecode Hospital Management System 1.0. Affected by this issue is some unknown functionality of the file /medicine.php. This manipulation of the argument editid causes sql injection. Remote exploitation of the attack is possible. The exploit has been published and may be used.	2026-07-04	6.3	CVE-2026-14619
itsourcecode--Hospital Management System	A flaw has been found in itsourcecode Hospital Management System 1.0. This affects an unknown function of the file /patient.php. This manipulation of the argument editid causes sql injection. The attack may be initiated remotely. The exploit has been published and may be used.	2026-07-04	6.3	CVE-2026-14638
itsourcecode--Hospital Management System	A vulnerability has been found in itsourcecode Hospital Management System 1.0. Impacted is an unknown function of the file /patientappointment.php. Such manipulation of the argument patiente leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2026-07-04	6.3	CVE-2026-14659
itsourcecode--Hospital Management System	A vulnerability has been found in itsourcecode Hospital Management System 1.0. Affected is an unknown function of the file /patientorder.php. Such manipulation of the argument editid leads to sql injection. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	2026-07-05	6.3	CVE-2026-14703
itsourcecode--Hospital Management System	A vulnerability was detected in itsourcecode Hospital Management System 1.0. The affected element is an unknown function of the file /patientlogin.php. Performing a manipulation of the argument loginid results in sql injection. Remote exploitation of the attack is possible. The exploit is now public and may be used.	2026-07-05	6.3	CVE-2026-14717
itsourcecode--Hospital Management System	A security flaw has been discovered in itsourcecode Hospital Management System 1.0. Affected by this issue is some unknown functionality of the file /patientprofile.php. Performing a manipulation of the argument patientname results in sql injection. The attack can be initiated remotely. The exploit has been released to the public and may be used for attacks.	2026-07-05	6.3	CVE-2026-14730
itsourcecode--Hospital	A weakness has been identified in itsourcecode Hospital Management System 1.0. This affects an unknown part of the file /patientreport.php.	2026-07-05	6.3	CVE-2026-14731

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	Executing a manipulation of the argument editid can lead to sql injection. The attack can be launched remotely. The exploit has been made available to the public and could be used for attacks.			
itsourcecode--Hospital Management System	A vulnerability was found in itsourcecode Hospital Management System 1.0. This affects an unknown function of the file /payment.php. The manipulation of the argument patientid results in sql injection. The attack can be launched remotely. The exploit has been made public and could be used.	2026-07-05	6.3	CVE-2026-14773
itsourcecode--Hospital Management System	A vulnerability was determined in itsourcecode Hospital Management System 1.0. This impacts an unknown function of the file /paymentdischarge.php. This manipulation of the argument patientid causes sql injection. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2026-07-05	6.3	CVE-2026-14774
itsourcecode--Online Hotel Management System	A vulnerability has been found in itsourcecode Online Hotel Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/mod_amenities/controller.php?action=add of the component POST Request Handler. The manipulation of the argument Name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2026-06-29	4.3	CVE-2026-13554
itsourcecode--Online Hotel Management System	A vulnerability was determined in itsourcecode Online Hotel Management System 1.0. This affects an unknown part of the file /admin/mod_users/controller.php?action=edit of the component POST Request Handler. This manipulation of the argument Name causes cross site scripting. The attack may be initiated remotely. The exploit has been publicly disclosed and may be utilized.	2026-06-29	4.3	CVE-2026-13556
itsourcecode--Online Hotel Management System	A vulnerability was identified in itsourcecode Online Hotel Management System 1.0. This vulnerability affects unknown code of the file /admin/mod_room/controller.php?action=add of the component POST Request Handler. Such manipulation of the argument Name leads to cross site scripting. The attack may be launched remotely. The exploit is publicly available and might be used.	2026-06-29	4.3	CVE-2026-13557
iv-org--Invidious	Invidious through 2.20260626.0, fixed in commit 77ad416, contains a broken object level authorization vulnerability that allows authenticated attackers to delete videos from other users' playlists by supplying an arbitrary global video index in the remove_video action of the playlist endpoint. Attackers can obtain per-video index values from the public playlist JSON API and submit them to the playlist video deletion endpoint without ownership validation, permanently removing videos from playlists they do not own.	2026-06-30	6.5	CVE-2026-58447
jetmonsters--Hotel Booking Lite	Subscriber Sensitive Data Exposure in Hotel Booking Lite <= 6.0.3 versions.	2026-07-02	6.5	CVE-2026-57347
jetmonsters--JetFormBuilder Dynamic Blocks Form Builder	The JetFormBuilder - Dynamic Blocks Form Builder plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.6.3. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to retrieve every distinct value stored under any arbitrary wp_postmeta key on the site - including WooCommerce	2026-07-02	5.3	CVE-2026-13459

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	billing PII such as <code>_billing_email</code> , <code>_billing_phone</code> , and <code>_billing_address</code> fields, order totals, attachment paths, and any third-party plugin credentials or tokens stored in post meta - provided at least one published JetFormBuilder form with a <code>get_from_db</code> generator field exists on the site. Exploitation requires that the target site has at least one published jet-form-builder post containing a field whose <code>generator_function</code> is set to <code>get_from_db</code> ; an attacker must supply a matching form ID, field name, and generator ID in the request, but all of these can be discovered by browsing the site's public forms.			
jetmonsters-- JetWidgets For Elementor	The JetWidgets For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to and including 1.0.21. This is due to insufficient output escaping and missing server-side validation of the Animated Box widget's <code>animation_effect</code> setting before it is rendered inside an HTML class attribute. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-01	6.4	CVE-2026-11380
jetmonsters-- MotoPress Appointment Booking	The MotoPress Appointment Booking plugin for WordPress is vulnerable to generic SQL Injection via the 's' parameter in all versions up to, and including, 2.4.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with custom-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires the <code>mpa_appointment_employee</code> custom role, meaning any user assigned this role can perform the attack.	2026-07-01	6.5	CVE-2026-13454
jetmonsters-- MotoPress Appointment Booking	The MotoPress Appointment Booking plugin for WordPress is vulnerable to Authorization Bypass Through User-Controlled Key in all versions up to, and including, 2.4.4. This is due to the <code>`POST /motopress/appointment/v1/bookings`</code> REST endpoint being registered with <code>`permission_callback` => `__return_true`</code> , allowing unauthenticated access, while the <code>`createBooking`</code> handler in <code>`BookingsRestController.php`</code> accepts an attacker-supplied <code>`payment_details.booking_id`</code> value and loads the referenced booking via <code>`findById()`</code> without verifying that the caller owns or has any rights to that booking. This makes it possible for unauthenticated attackers to overwrite the customer name, email address, phone number, and <code>`customer_id`</code> of any non-confirmed victim booking by submitting a request with no reservation items, causing <code>`BookingService::createBooking()`</code> to load the existing victim booking object and persist it with attacker-controlled customer data. Victim booking IDs can be harvested prior to exploitation without authentication by querying the also-publicly-accessible <code>`GET /motopress/appointment/v1/bookings/reservations`</code> endpoint with a guessable <code>`service_id`</code> and date range, and only bookings whose status is not <code>`STATUS_CONFIRMED`</code> (e.g., pending or auto-draft) are valid targets.	2026-07-03	5.3	CVE-2026-9180
jgwhite33--WP Google Review Slider	The Wp Google Places Review Slider plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'place' parameter in versions up to, and including, 18.1. This is due to insufficient input sanitization and output escaping in <code>admin/partial/googlecrawl_dfs.php</code> , where the <code>\$_GET['place']</code> value is URL-decoded, <code>stripslashes()</code> 'd, and echoed directly into an HTML value attribute with no <code>esc_attr()</code> call when the supplied place is not	2026-07-01	6.1	CVE-2026-13015

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	already a stored key in the wprev_google_crawls option. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a specially crafted link.			
joedolson--My Calendar Accessible Event Manager	The My Calendar - Accessible Event Manager plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 3.7.14 via the 'vcal' parameter due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to enumerate occurrence IDs and access the full iCalendar export of non-public, draft, trashed, and personal calendar events, disclosing sensitive event metadata including titles, descriptions, dates, locations, organizer and host details, permalinks, and related calendar metadata.	2026-07-02	5.3	CVE-2026-11896
Keksdieb--ez Form Calculator Premium	Unauthenticated Broken Access Control in ez Form Calculator Premium <= 2.14.1.2 versions.	2026-07-02	5.3	CVE-2026-57750
kirilkirkov--Ecommerce-Codelgniter-Bootstrap	A weakness has been identified in kirilkirkov Ecommerce-Codelgniter-Bootstrap up to 23105f25dadf57b4314fc015a63a7c6e910c89df. Impacted is the function do_upload_others_images of the file application/modules/vendor/controllers/AddProduct.php of the component Vendor Image Manager. Executing a manipulation of the argument folder can lead to path traversal. It is possible to launch the attack remotely. This product takes the approach of rolling releases to provide continuous delivery. Therefore, version details for affected and updated releases are not available. This patch is called de1c9e73ccf3bd032d9a0525c4752290d959dd8b. It is best practice to apply a patch to resolve this issue.	2026-07-04	5.4	CVE-2026-14636
kirilkirkov--Ecommerce-Codelgniter-Bootstrap	A vulnerability was found in kirilkirkov Ecommerce-Codelgniter-Bootstrap up to 95dfa8cebbb87ab46ae450643a07241274a74dce. Affected by this issue is the function setReferrer of the file application/core/MY_Controller.php of the component Trusted Backend Interface. The manipulation of the argument href results in open redirect. The attack can be executed remotely. The exploit has been made public and could be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The patch is identified as 213babdbaa949e94557246414db0130e01394517. A patch should be applied to remediate this issue.	2026-07-04	4.3	CVE-2026-14632
kirilkirkov--Ecommerce-Codelgniter-Bootstrap	A vulnerability was determined in kirilkirkov Ecommerce-Codelgniter-Bootstrap up to 49b20f53de2b7ec34e920b11c863f1491d911a04. This affects an unknown part of the file /index.php/api/product/set of the component Hidden REST API Endpoint. This manipulation of the argument title/description causes cross site scripting. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. Patch name: d9785f995da77bdc62fb2d34bad5f7a162c9ad23. To fix this issue, it is recommended to deploy a patch.	2026-07-04	4.3	CVE-2026-14633

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kirilkirkov--Ecommerce-CodeIgniter-Bootstrap	A vulnerability was identified in kirilkirkov Ecommerce-CodeIgniter-Bootstrap up to 213babdbaa949e94557246414db0130e01394517. This vulnerability affects the function checkForPostRequests of the file application/core/MY_Controller.php of the component Subscribed Emails Admin Page. Such manipulation of the argument User-Agent leads to cross site scripting. The attack may be performed from remote. The exploit is publicly available and might be used. This product utilizes a rolling release system for continuous delivery, and as such, version information for affected or updated releases is not disclosed. The name of the patch is 23105f25dadf57b4314fc015a63a7c6e910c89df. It is advisable to implement a patch to correct this issue.	2026-07-04	4.3	CVE-2026-14634
kodezen--Academy LMS WordPress LMS Plugin for Complete eLearning Solution	The Academy LMS - WordPress LMS Plugin for Complete eLearning Solution plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to, and including, 3.8.1. This is due to the '/topics' REST API endpoint being registered with a permission callback set to '__return_true', allowing unauthenticated access to course curriculum data without verifying the course's post status or user enrollment. This makes it possible for unauthenticated attackers to access detailed curriculum information for private, draft, scheduled, or password-protected courses by enumerating course IDs.	2026-07-02	5.3	CVE-2026-5348
latepoint--LatePoint Calendar Booking Plugin for Appointments and Events	The LatePoint - Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 5.6.1. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to modify the personally identifiable information (first name, last name, phone number, and notes) of any existing customer record, including those linked to administrator accounts, by submitting the booking form with a known customer's email address. Exploitation requires the plugin to be configured with guest bookings enabled (is_customer_auth_disabled() returning true), which is necessary for the vulnerable unauthenticated code path in process_step_customer() to be reached.	2026-07-03	5.3	CVE-2026-11398
latepoint--LatePoint Calendar Booking Plugin for Appointments and Events	The LatePoint - Calendar Booking Plugin for Appointments and Events plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 5.6.2 via the 'service_id' parameter due to missing validation on a user controlled key. This makes it possible for unauthenticated attackers to create approved bookings against services explicitly restricted to admins and agents, consuming restricted appointment capacity and triggering unauthorized bookings for admin/agent-only services. The bypass works via both the params[booking][service_id] parameter in steps__load_step and the presets[selected_service] parameter in steps__start, both of which are publicly accessible without authentication.	2026-07-02	5.3	CVE-2026-12657
LibrePhotos--librephotos	LibrePhotos before 1.0.0 contains a broken object level authorization vulnerability in the SetPhotosShared endpoint that allows authenticated users to grant themselves access to other users' private photos by bypassing ownership validation. Attackers can manipulate shared_to relations without proper owner checks to read arbitrary private photos belonging to other users.	2026-06-29	5.9	CVE-2026-57943

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
LibreTranslate-- LibreTranslate	LibreTranslate through 1.9.7, fixed in commit 397fd22, contains an IP spoofing vulnerability in the get_remote_address() function that allows unauthenticated attackers to spoof client IP addresses by injecting arbitrary values into the X-Forwarded-For header without trusted proxy validation. Attackers can bypass per-IP rate limiting and flood bans by supplying forged addresses in the X-Forwarded-For header to enable unlimited API abuse.	2026-06-29	5.3	CVE-2026-57942
LinkWhisper-- Link Whisper Premium	Subscriber Broken Access Control in Link Whisper Premium <= 2.9.0 versions.	2026-07-02	6.5	CVE-2026-57353
Livemesh-- Livemesh Addons for WPBakery Page Builder	Contributor Cross Site Scripting (XSS) in Livemesh Addons for WPBakery Page Builder <= 3.9.4 versions.	2026-07-02	6.5	CVE-2026-57754
lobehub-- lobehub	LobeChat before version 2.2.10-canary.15 contains a regular expression denial of service (ReDoS) vulnerability that allows authenticated attackers to block the Node.js event loop by supplying a catastrophic-backtracking pattern in a GitHub repository URL path during skill import. Attackers can craft a malicious basePath value containing unescaped regex metacharacters such as catastrophic-backtracking patterns, which are injected into a dynamically constructed regular expression in the findSkillMd function and executed synchronously against archive entries, denying service to all concurrent users for tens of seconds per request.	2026-07-02	6.5	CVE-2026-58578
lobehub-- lobehub	LobeChat through 2.2.9 contains a broken access control vulnerability in the retrieval-augmented-generation semantic search functionality that allows authenticated attackers to access other users' data by exploiting missing user-identifier predicates in the chunk model semanticSearch method. Attackers can supply arbitrary victim file or knowledge-base identifiers through the chunk retrieval and chat knowledge-base paths to retrieve text content, file names, and metadata belonging to other users.	2026-07-02	6.5	CVE-2026-59098
lobehub-- lobehub	LobeChat through 2.2.9 server-database deployments are vulnerable to broken object-level authorization in MessageModel. The updateMessagePlugin, updatePluginState, updatePluginError, updateTTS and updateTranslate methods filter target rows by message id alone, omitting the userId scope that sibling methods apply, and findMessagePlugin reads back by id alone. Reachable via the corresponding tRPC message procedures, an authenticated user who knows another user's message identifier can overwrite that victim's plugin tool-call metadata, plugin state/error, text-to-speech and translation records on the same instance, and the tampered content is served back to the victim. Exploitation requires knowledge of the victim's non-enumerable message identifier.	2026-07-02	5.9	CVE-2026-58580
lobehub-- lobehub	LobeChat through 2.2.9 contains a broken object level authorization vulnerability that allows authenticated attackers to access and modify other users' chat-group agent data by supplying arbitrary group identifiers. Attackers can invoke the getGroupAgents, updateAgentInGroup, and removeAgentsFromGroup operations without user-scoped predicates to	2026-07-02	5	CVE-2026-59100

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	read agent listings, modify agent roles and ordering, and remove agents from chat groups belonging to other users.			
mainwp--MainWP	Subscriber Broken Access Control in MainWP <= 6.1.1 versions.	2026-06-29	6.3	CVE-2026-57327
Matteo Manna--Simple User Avatar	Authorization Bypass Through User-Controlled Key vulnerability in Matteo Manna Simple User Avatar allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Simple User Avatar: from n/a through 4.9.	2026-06-29	4.3	CVE-2026-57676
Microsoft--Azure Synapse	Improper access control in Azure Synapse allows an authorized attacker to elevate privileges over a network.	2026-07-02	4.8	CVE-2026-26145
Microsoft--Microsoft Edge (Chromium-based)	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2026-07-03	6.5	CVE-2026-45489
Microsoft--Microsoft Edge (Chromium-based)	Exposure of sensitive information to an unauthorized actor in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-07-03	6.5	CVE-2026-56646
Microsoft--Microsoft Edge (Chromium-based)	Server-side request forgery (ssrf) in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-07-03	6.5	CVE-2026-57987
Microsoft--Microsoft Edge (Chromium-based)	Operation on a resource after expiration or release in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	2026-07-03	6.1	CVE-2026-58291
Microsoft--Microsoft Edge (Chromium-based)	Absolute path traversal in Microsoft Edge for Android allows an unauthorized attacker to disclose information locally.	2026-07-03	6.2	CVE-2026-58300
Microsoft--Microsoft Edge (Chromium-based)	Relative path traversal in Microsoft Edge for Android allows an unauthorized attacker to disclose information locally.	2026-07-03	6.8	CVE-2026-58522
Microsoft--Microsoft Edge (Chromium-based)	Improper access control in Microsoft Edge for Android allows an unauthorized attacker to bypass a security feature over a network.	2026-07-03	6.5	CVE-2026-58523
Microsoft--Microsoft Edge (Chromium-based)	User interface (ui) misrepresentation of critical information in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-07-03	5.4	CVE-2026-45488
Microsoft--Microsoft Edge	Server-side request forgery (ssrf) in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-07-03	5.4	CVE-2026-58278

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
(Chromium-based)				
Microsoft--Microsoft Edge (Chromium-based)	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-07-03	5.4	CVE-2026-58524
Microsoft--Microsoft Edge (Chromium-based)	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Edge (Chromium-based) allows an authorized attacker to disclose information locally.	2026-07-03	4.2	CVE-2026-55945
Microsoft--Microsoft Edge (Chromium-based)	Insufficient ui warning of dangerous operations in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-07-03	4.3	CVE-2026-58597
Misbah WP--Mosaic Gallery - Advanced Gallery	Contributor Cross Site Scripting (XSS) in Mosaic Gallery – Advanced Gallery <= 1.2.0 versions.	2026-07-02	6.5	CVE-2026-57755
mjperpinosa--stumasy	A weakness has been identified in mjperpinosa stumasy up to 327d1b0f2915ba79d7ef8ebb74553e987609d9be. The impacted element is the function Notes_controller::search_scratch_data of the file application/PHP/objects/notes/search_scratch_data.php. This manipulation of the argument field_name causes sql injection. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The project was informed of the problem early through an issue report but has not responded yet.	2026-07-05	6.3	CVE-2026-14751
n8n--n8n	n8n before 2.8.0 contains an authentication bypass vulnerability allowing authenticated SSO users to disable SSO enforcement through the API. Attackers can create local password credentials to authenticate directly, bypassing organizational SSO policies and identity-provider-enforced multi-factor authentication.	2026-06-30	6.3	CVE-2026-56350
n8n--n8n	n8n contains a stored cross-site scripting vulnerability in the Chat Trigger node's Custom CSS field due to a misconfiguration of the sanitize-html library. Affected releases are those before 1.123.27, the 2.0.0 through 2.13.2 line, and 2.14.0 (fixed in 1.123.27, 2.13.3, and 2.14.1). An authenticated user with permission to create or modify workflows can inject JavaScript that bypasses sanitization, resulting in stored XSS against any user who visits the public chat page.	2026-06-30	5.4	CVE-2026-56356
n8n--n8n	n8n before 2.25.7 and 2.26.x before 2.26.2 contains an abstract syntax tree (AST) security validator bypass in the Python Code node. An authenticated user with permission to create or modify workflows containing a Python Code node can bypass the validator and access the task executor module namespace. The issue only affects self-hosted instances where the Python Task Runner is enabled; where	2026-06-30	5	CVE-2026-56777

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	N8N_BLOCK_RUNNER_ENV_ACCESS is configured to allow it, this can disclose environment variables accessible to the task runner process.			
Nathanbarry--Kit (formerly ConvertKit) for WooCommerce	Unauthenticated Sensitive Data Exposure in Kit (formerly ConvertKit) for WooCommerce <= 2.1.5 versions.	2026-07-02	5.3	CVE-2026-57753
nesquena--hermes-webui	Hermes WebUI before 0.51.521 validates the workspace of an imported session under the active named profile but constructs the Session object without setting its profile in the /api/session/import handler, so the imported session is persisted with a null profile. Because a null profile is treated as the default profile by the profile authorization check, a user on the default profile can export the imported session transcript and use its session identifier to read files from the named profile's workspace, defeating the application's profile isolation.	2026-06-30	6.5	CVE-2026-58174
netdata--netdata	Netdata before 2.3.1 reflects the user-supplied love query parameter of the api/v2/ilove.svg and api/v3/ilove.svg endpoints verbatim into the generated SVG document (into a text element) without HTML or XML escaping, and serves the response with Content-Type image/svg+xml. An attacker can craft a URL such as /api/v2/ilove.svg?love=<script>...</script>; when a victim navigates to it the injected script executes in the victim browser in the origin of the Netdata instance (reflected cross-site scripting). These endpoints are registered with HTTP_ACL_NOCHECK and anonymous access and, because bearer-token protection is disabled by default, are reachable without authentication on a default Netdata agent. The issue was resolved by removing the ilove endpoint.	2026-07-02	6.1	CVE-2025-71385
nextlevelbuilder-GoClaw	A security vulnerability has been detected in nextlevelbuilder GoClaw up to 3.13.0-beta.2. Impacted is the function MethodRouter.Handle of the file internal/gateway/router.go of the component WebSocket RPC Handler. Such manipulation leads to incorrect authorization. The attack may be launched remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report.	2026-07-05	6.3	CVE-2026-14716
nikhilgadhiya--Product Video Gallery for Woocommerce	The Product Video Gallery for Woocommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via custom_thumbnail Parameter in all versions up to, and including, 1.5.1.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with shop manager-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-02	4.4	CVE-2026-10104
NousResearch--hermes-agent	A security flaw has been discovered in NousResearch hermes-agent up to 0.15.2. The affected element is the function shell.exec of the file tui_gateway/server.py. The manipulation results in protection mechanism failure. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-07-04	6.3	CVE-2026-14625
NousResearch--hermes-agent	A security vulnerability has been detected in NousResearch hermes-agent up to 0.15.2. This affects the function DiscordAdapter._is_allowed_user of the file gateway/platforms/discord.py of the component Discord Platform Integration. Such manipulation leads to improper authentication. The	2026-07-04	5.6	CVE-2026-14627

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attack can be launched remotely. This attack is characterized by high complexity. The exploitability is reported as difficult. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.			
NousResearch--hermes-agent	A vulnerability was detected in NousResearch hermes-agent up to 2026.5.16. This impacts the function extract_media of the file gateway/platforms/base.py of the component Live Webhook Endpoint. Performing a manipulation results in path traversal. The attack may be initiated remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-07-04	5.3	CVE-2026-14628
NousResearch--hermes-agent	A weakness has been identified in NousResearch hermes-agent up to 2026.4.30. The impacted element is the function AIAgent.run_conversation of the file run_agent.py of the component HTTP API. This manipulation of the argument todos causes denial of service. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-07-04	4.3	CVE-2026-14626
NousResearch--hermes-agent	A vulnerability was determined in NousResearch hermes-agent 2026.5.29.2. The impacted element is the function skill_view of the file tools/skills_tool.py. Executing a manipulation of the argument Name can lead to path traversal. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. This patch is called 56f833efa427ccb444c0f9ad1759af1012f2124d. It is advisable to implement a patch to correct this issue.	2026-07-05	4.3	CVE-2026-14783
NVIDIA--Triton Inference Server	NVIDIA Triton Inference Server for Linux contains a vulnerability where an attacker can cause a use-after-free issue. A successful exploit of this vulnerability might lead to denial of service.	2026-07-01	5.9	CVE-2026-24266
octagonwebstudio--Premium Addons for KingComposer	The Premium Addons for KingComposer plugin for WordPress is vulnerable to unauthorized modification and loss of data in versions up to, and including, 1.1.1. This is due to missing authorization and capability checks on the add_custom_sidebar() and remove_custom_sidebar() AJAX handlers, both of which are exposed through wp_ajax_nopriv_* hooks and write directly to the octagon_custom_sidebar option via update_option(). This makes it possible for unauthenticated attackers to create arbitrary custom widget areas or delete existing custom sidebars, which can cause widgets assigned to those areas to silently lose their registration and stop rendering.	2026-06-30	5.3	CVE-2026-12349
ohler55--oj	Oj (Optimized JSON) is a JSON parser and Object marshaller packaged as a Ruby gem. In versions prior to 3.17.3, Oj.load in :object mode reads uninitialized stack memory (and, for long keys, reads out of bounds) when parsing a JSON object whose key is 254 bytes or longer. The interned bytes can surface to the caller, disclosing process stack memory. In ext/oj/intern.c, form_attr() handles the long-key path by allocating a heap buffer, `b`, populating it with the attribute name, and then freeing it - but it passed the uninitialized stack buffer buf (not b) to rb_intern3(). rb_intern3 therefore reads len + 1 bytes of uninitialized stack memory. When the key length is >= 256, it also reads out of bounds past the 256-byte buf. The resulting bytes are interned and can reach the caller via the produced Symbol or via the EncodingError message raised on invalid UTF-	2026-06-30	5.3	CVE-2026-54500

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	8, leaking process stack contents. This issue has been fixed in version 3.17.3.			
omec-project--amf	A vulnerability was determined in omec-project amf up to 2.1.1. This issue affects the function RRCInactiveTransitionReport of the component NGAP Message Handler. Executing a manipulation can lead to denial of service. The attack may be performed from remote. The exploit has been publicly disclosed and may be utilized. This patch is called 34bc6724acc97dba1f8691e586da95b042cb612d. A patch should be applied to remediate this issue.	2026-07-04	4.3	CVE-2026-14623
omec-project--amf	A vulnerability was identified in omec-project amf up to 2.0.2/2.1.1. Impacted is an unknown function of the file /go/src/amf/ngap/handler.go of the component NGSetupRequest Handler. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit is publicly available and might be used. The identifier of the patch is 34bc6724acc97dba1f8691e586da95b042cb612d. To fix this issue, it is recommended to deploy a patch.	2026-07-04	4.3	CVE-2026-14624
onnx--onnx	A weakness has been identified in onnx up to 1.21.x. This vulnerability affects the function convPoolShapeInference_opset19 of the file onnx/defs/nn/old.cc of the component onnxruntime. This manipulation causes out-of-bounds read. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. Patch name: a7bf3a0f1d18bb62575236ef6e4944980c40e045. It is recommended to apply a patch to fix this issue.	2026-07-04	4.3	CVE-2026-14647
opajaap--WP Photo Album Plus	The WP Photo Album Plus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'subtext' parameter in all versions up to, and including, 9.1.13.005 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. A contributor-level attacker can embed the malicious [photo] shortcode in a post submitted for review, causing the stored payload to execute when an administrator or any other user views the post.	2026-07-01	6.4	CVE-2026-10095
Open Asset Import Library--Assimp	A vulnerability was determined in Open Asset Import Library Assimp up to 6.0.4. Affected is the function Assimp::Exporter::ExportToBlob of the file code/AssetLib/Ply/PlyLoader.cpp of the component PLY Model Handler. This manipulation causes double free. The attack can be initiated remotely. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report.	2026-07-03	6.3	CVE-2026-14604
Open Asset Import Library--Assimp	A security vulnerability has been detected in Open Asset Import Library Assimp up to 5.4.3. Affected by this vulnerability is the function Assimp::SceneCombiner::Copy of the file code/Common/SceneCombiner.cpp of the component Model File Handler. Such manipulation of the argument width/height leads to heap-based buffer overflow. An attack has to be approached locally. The exploit has been disclosed publicly and may be used. This and similar defects are tracked and handled via issue #6128.	2026-07-01	5.3	CVE-2025-15666

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Open Asset Import Library--Assimp	A flaw has been found in Open Asset Import Library Assimp up to 6.0.5. Impacted is the function Assimp::CSMImporter::InternReadFile of the file code/AssetLib/CSM/CSMLoader.cpp of the component CSM File Handler. This manipulation causes heap-based buffer overflow. The attack is restricted to local execution. The exploit has been published and may be used. Patch name: eb84eec580d3f4ba2f0fd87409b7d0744620f11e. Applying a patch is the recommended action to fix this issue.	2026-07-03	5.3	CVE-2026-14610
open-telemetry--opentelemetry-java-instrumentation	OpenTelemetry Java Instrumentation provides OpenTelemetry auto-instrumentation and instrumentation libraries for Java. In versions prior to 2.28.0, the JDBC auto-instrumentation may fail to sanitize passwords in SQL CONNECT statements when the password is double-quoted. As a result, clear-text database passwords can be added to trace span attributes and exported to observability backends. This issue has been fixed in version 2.28.0.	2026-07-01	6.5	CVE-2026-54704
open-telemetry--opentelemetry-java-instrumentation	OpenTelemetry Java Instrumentation provides OpenTelemetry auto-instrumentation and instrumentation libraries for Java. In versions prior to 2.27.0, the RMI context propagation payload reader limits the number of context entries but does not limit the aggregate size of the strings read from the stream. An attacker who can reach an RMI endpoint on an instrumented JVM can send an oversized context propagation payload. This can cause excessive memory allocation while the JVM reads the payload, potentially leading to denial of service. The issue affects only deployments where RMI instrumentation is enabled and an RMI endpoint is network-reachable. This issue has been fixed in version 2.27.0.	2026-07-01	5.3	CVE-2026-54712
open-webui--open-webui	Open WebUI before 0.6.27 contains a server-side request forgery vulnerability in the /api/v1/retrieval/process/web endpoint that allows authenticated users to bypass SSRF protections. Attackers can manipulate URL parameters with location redirect headers to access internal services and potentially execute commands via instance secrets.	2026-06-30	5	CVE-2026-56399
Open5GS--Open5GS	A vulnerability was detected in Open5GS up to 2.7.7. Affected by this vulnerability is the function amf_nnrf_handle_nf_discover of the file src/amf/nnrf-handler.c of the component AMF. The manipulation results in denial of service. The attack may be launched remotely. The exploit is now public and may be used. The patch is identified as fb5f67703de0213fb9c6e6ef3b48b6c1707e9503. It is best practice to apply a patch to resolve this issue.	2026-07-04	4.3	CVE-2026-14618
openGauss-server--openGauss-server-7.0.0-RC2	See CVE Link for Additional Details	2026-06-30	5.9	CVE-2026-14178
Paolo--GeoDirectory	Subscriber Server Side Request Forgery (SSRF) in GeoDirectory <= 2.8.161 versions.	2026-07-02	6.4	CVE-2026-57681
papermark--papermark	Papermark through 0.22.0 contains a cross-origin resource sharing (CORS) misconfiguration vulnerability that allows unauthenticated remote attackers to perform credentialed cross-origin requests by exploiting the TUS-based viewer upload endpoint reflecting arbitrary request Origins with Access-Control-Allow-Credentials set to true. Attackers can lure authenticated victims to malicious pages that silently issue credentialed	2026-06-29	4.7	CVE-2026-57957

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cross-origin requests to upload arbitrary files into victim datarooms and read credentialed responses.			
parorrey--JSON API User	The JSON API User plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'content' parameter of the post_comment API endpoint in versions up to, and including, 4.1.0 This is due to insufficient input sanitization in the post_comment() function, which passes the attacker-controlled comment_content value directly to wp_insert_comment() without applying any HTML sanitization, and additionally allows the caller to set comment_approved=1 to self-approve the comment and bypass moderation. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-03	6.4	CVE-2026-9626
parseablehq--parseable	Parseable before 2.9.2 contains an information disclosure vulnerability in the notification-target API endpoints that returns webhook tokens and basic-auth credentials in cleartext due to commented-out secret-masking functionality. Any authenticated user with the GetAlert action, including low-privilege reader roles, can recover credentials and internal endpoint URLs for all configured notification targets by querying GET /api/v1/targets or related endpoints.	2026-06-29	6.5	CVE-2026-56783
photoprism--photoprism	PhotoPrism before 260601-a7d098548 contains a broken access control vulnerability that allows authenticated non-admin users to modify other users' profile information by sending requests to arbitrary user endpoints. Attackers can exploit the missing session-to-user identifier validation in the PUT users API endpoint to overwrite another user's profile details without authorization.	2026-06-29	4.3	CVE-2026-57945
php--php	In PHP versions 8.2.* before 8.2.32, 8.3.* before 8.3.32, 8.4.* before 8.4.23, 8.5.* before 8.5.8, the AES-WRAP-PAD algorithm implementation in OpenSSL extension contains a buffer allocation flaw. The output buffer for the AES key-wrap-with-padding operation is sized from the plaintext length without accounting for RFC 5649 expansion. This may cause OpenSSL to write beyond allocated memory, corrupting heap metadata and triggering application abort.	2026-07-03	5.6	CVE-2026-14355
pinpoint-apm--pinpoint	Pinpoint through version 3.1.0 contains an insecure session management vulnerability that allows attackers to access the pinpointJwt session cookie due to missing HttpOnly and Secure attributes, enabling JavaScript access via document.cookie and cleartext transmission over HTTP. Attackers can exploit stored or reflected cross-site scripting vulnerabilities to exfiltrate the session token or intercept it through network sniffing to perform session hijacking.	2026-06-29	6.8	CVE-2026-57948
PraisonAI--PraisonAI	PraisonAI before 0.1.7 fails to validate that project_id in issue create and update request bodies belongs to the URL workspace. An attacker can create issues referencing projects from other workspaces, causing cross-tenant data pollution in project statistics aggregation without workspace constraints.	2026-07-02	4.3	CVE-2026-58653
presenton--presenton	Presenton before 0.8.8-beta bundles an MCP server that, on server/Docker deployments configured with session authentication (AUTH_USERNAME/AUTH_PASSWORD), is reachable unauthenticated at /mcp because the nginx front-end does not apply the auth_request gate to that path and the MCP server auto-mints a valid internal session token for	2026-06-30	6.5	CVE-2026-58446

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the configured user. A remote unauthenticated attacker can invoke MCP tools such as generate_presentation, performing authenticated application actions, consuming the operators configured LLM API keys, and creating presentations in the operators instance. The Electron desktop build is not affected (MCP disabled).			
properfraction--CrawlWP SEO	Cross-Site Request Forgery (CSRF) vulnerability in properfraction CrawlWP SEO allows Cross Site Request Forgery. This issue affects CrawlWP SEO: from n/a through 3.0.16.	2026-07-05	4.3	CVE-2026-59520
propertyhive--Houzez Property Feed	The Houzez Property Feed plugin for WordPress is vulnerable to SQL Injection via the 'orderby' parameter in all versions up to, and including, 2.5.46 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query in the prepare_items() method of the Houzez_Property_Feed_Admin_Logs_Export_Table (and Houzez_Property_Feed_Admin_Logs_Import_Table) class. The user-controlled \$_GET['orderby'] and \$_GET['order'] values are filtered only with sanitize_text_field() and then concatenated into the SQL format string before \$wpdb->prepare() is called - prepare() only parameterizes the appended LIMIT/OFFSET clause and cannot retroactively secure the already-tainted ORDER BY clause. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-07-02	4.9	CVE-2026-13357
qodeinteractive--Qi Blocks	The Qi Blocks plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.4.9 via the 'page_id' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with author-level access and above, to modify the stored Qi Blocks styles of arbitrary posts, templates, or widgets they do not own - including site-wide surfaces via the reserved 'template' and 'widget' page_id values - enabling unauthorized frontend defacement, content hiding, and degradation of any page on the site. The endpoint's permission_callback checks only the generic edit_posts and publish_posts capabilities, meaning any user with the built-in Author role satisfies the check regardless of post ownership.	2026-07-01	4.3	CVE-2026-10096
radareorg--radare2	A vulnerability was determined in radareorg radare2 up to 6.1.6. This affects the function core_anal_bytes of the file libr/core/cmd_anal.inc. This manipulation causes integer overflow. The attack needs to be launched locally. The exploit has been publicly disclosed and may be utilized. It is suggested to install a patch to address this issue.	2026-07-05	5.3	CVE-2026-14757
RadiusTheme--Classified Listing	Subscriber Broken Access Control in Classified Listing <= 5.4.2 versions.	2026-07-02	6.5	CVE-2026-57355
Raera - Ankara Web Design and Digital Advertising Agency--Destekz	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Raera - Ankara Web Design and Digital Advertising Agency Destekz allows Reflected XSS. This issue affects Destekz: through 02062026. NOTE: The vendor was contacted and it was learned that the product is not supported.	2026-07-03	6.1	CVE-2026-4322
Red Hat--Red Hat Build of Keycloak	A flaw was found in the Identity Provider (IdP) mapper component of Keycloak, which is used to manage how user information from external services is mapped to Keycloak users. An administrator with limited	2026-06-30	6.5	CVE-2026-12388

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	permissions to manage identity providers can exploit this flaw by creating a "Hardcoded Role" mapper that assigns high-level administrative roles (like realm-admin) to themselves or others. This allows a restricted administrator to bypass security checks and gain full control over the entire realm.			
Red Hat--Red Hat Build of Keycloak	A flaw was found in Keycloak. A highly privileged user with `manage-clients` permission can exploit this vulnerability by injecting a hardcoded role mapper into any client. This action allows the user to bypass existing scope restrictions and inject the `realm-admin` role into generated tokens, resulting in privilege escalation and full administrative access to the realm.	2026-06-30	6.5	CVE-2026-4629
Red Hat--Red Hat Build of Keycloak	A flaw was found in the ClientResource component of Keycloak's admin services when Fine-Grained Admin Permissions (FGAP) v2 is enabled. This issue allows a delegated administrator, who should only have limited control over specific clients, to attach or remove hidden client scopes that they are not authorized to see or manage. As a result, an attacker could inject unauthorized data or permissions into the security tokens issued to end-users, potentially tricking other applications into granting higher levels of access than intended.	2026-07-03	5.4	CVE-2026-14614
Red Hat--Red Hat Build of Keycloak	A vulnerability was discovered in Keycloak's Admin UI extension that allows certain administrative users to bypass security restrictions. When Fine-Grained Admin Permissions (FGAPv2) are enabled, an administrator who should only be able to search for users (but not view their full details) can use a specific "brute-force-user" endpoint to access a user's full profile. This includes sensitive information and security metadata. The issue occurs because the system fails to check if the administrator has the required "view" permission for that specific user when using this particular search path.	2026-06-30	4.3	CVE-2026-14209
Red Hat--Red Hat Build of Keycloak	A vulnerability was discovered in Keycloak's administrative interface that allows certain administrators to see information about groups they shouldn't have access to. When the new Fine-Grained Admin Permissions (FGAP v2) are turned on, an administrator who is allowed to see a specific "role" can also see a list of all groups assigned to that role. The system fails to check if the administrator has permission to see those specific groups. This could allow a restricted administrator to discover "hidden" groups and see their details, such as internal names and custom settings, which might contain sensitive deployment information.	2026-07-03	4.3	CVE-2026-14613
Red Hat--Red Hat Build of Keycloak	A flaw was found in the Fine-Grained Admin Permissions (FGAP) v2 implementation within Keycloak's administrative services. When FGAP v2 is enabled, the system fails to properly filter child groups based on the caller's specific permissions when requested through a parent group. This allows a delegated administrator to view details of child groups they are not authorized to access directly, including group names, paths, and custom attributes.	2026-07-03	4.3	CVE-2026-14615
Red Hat--Red Hat Build of Keycloak	A flaw exists in the org.keycloak.broker.oidc package where the OIDC broker incorrectly synchronizes the email_verified claim. When an OIDC identity provider is configured with trustEmail=true and the userinfo endpoint is enabled, Keycloak retrieves the email address from the userinfo response but retrieves the email_verified status exclusively from the id_token. The root cause is a lack of validation ensuring that the	2026-07-05	4.8	CVE-2026-14781

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	email_verified claim in the id_token actually refers to the email address returned by the userinfo endpoint. If these two sources return different email addresses, the id_token's email_verified=true claim is blindly applied to the userinfo email. Exploitation Conditions: The OIDC identity provider must have trustEmail set to true (non-default). The userinfo endpoint must be enabled (default). The attacker must control or have compromised the upstream OIDC provider. Concrete Impact: Mark arbitrary email addresses as verified in the Keycloak database. Bypass email-based security controls or verification workflows. Potential account takeover if the application relies solely on the email_verified flag from the IdP to link accounts.			
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in sssd. When authenticating with a YubiKey, the SSSD PAM responder can crash due to a use-after-free vulnerability, where a memory pointer is incorrectly handled. A local attacker could exploit this flaw by manipulating smartcard or YubiKey contents, leading to a denial of service that disrupts authentication. This vulnerability also presents a potential for privilege escalation, although it is difficult to exploit.	2026-06-30	6.4	CVE-2026-12610
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in p11-kit. The RPC message attribute parsing functions p11_rpc_message_get_attribute() and p11_rpc_message_get_attribute_array_value() form a mutually-recursive call chain with no recursion depth limit when processing nested CKA_WRAP_TEMPLATE, CKA_UNWRAP_TEMPLATE, and CKA_DERIVE_TEMPLATE attributes. An unauthenticated attacker with local access to the p11-kit RPC Unix domain socket can send a specially crafted request with deeply nested template attributes, causing stack exhaustion and crashing the p11-kit server process and its dependent services.	2026-06-29	6.2	CVE-2026-13757
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in dhcpcd's IPv6 Neighbor Discovery Router Advertisement processing. A specially crafted IPv6 Router Advertisement containing a zero-length Neighbor Discovery option can bypass validation during packet storage and later be reparsed without adequate validation, causing the parser to enter a non-advancing loop. Successful exploitation may result in excessive CPU consumption, leading to a denial of service.	2026-07-01	6.5	CVE-2026-14258
Red Hat--Red Hat Enterprise Linux 10	RAOP module accepts unbounded Content-Length values and does not check the pw_array_add() return.	2026-07-01	6.5	CVE-2026-14324
Red Hat--Red Hat Enterprise Linux 10	Multiple unbounded alloca() calls in the PulseAudio protocol server.	2026-07-01	5.5	CVE-2026-14330
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in spice-vdagent. A malicious or compromised SPICE host can trigger an integer overflow by sending a specially crafted message. This vulnerability can lead to a heap buffer overflow, causing the spice-vdagent daemon to crash and resulting in a Denial of Service (DoS) for the virtual machine. This issue requires the SPICE host to be untrusted or compromised for exploitation.	2026-06-29	5.1	CVE-2026-57965
Red Hat--Red Hat Enterprise Linux 10	Two off-by-one errors in the FreeIPA ipa-otpd daemon's OAuth2 device authorization handler can cause out-of-bounds memory access when processing an oversized response from a configured external OAuth2/OIDC Identity Provider. An attacker who controls or can man-in-the-middle the IdP endpoint may be able to trigger ipa-otpd to write or read one byte past the end of a fixed-size buffer. Exploitation requires FreeIPA to be	2026-07-03	4.2	CVE-2026-14612

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	configured with an external IdP, attacker control or MITM of that IdP, and a user to initiate the OAuth2 device authorization flow. The most likely impact is limited denial of service affecting the ipa-otpd daemon.			
Red Hat--Red Hat Enterprise Linux 10	A path traversal vulnerability was found in spice-vdagent. This flaw allows a malicious or compromised SPICE host to write arbitrary files to any location on the guest operating system. This occurs because the filename provided by the SPICE host during file transfers is not properly sanitized before being used. An attacker could exploit this to write to sensitive locations with the privileges of the spice-vdagent process, typically the logged-in user. This issue requires the SPICE host to be untrusted or compromised for exploitation.	2026-06-29	4.4	CVE-2026-57966
Red Hat--Red Hat Enterprise Linux 6	A flaw was found in GIMP's PSP file format parser. A double-free condition occurs in the read_layer_block() function when processing a specially crafted PSP file. This could allow an attacker to cause memory corruption, potentially leading to denial of service or arbitrary code execution.	2026-07-02	6.1	CVE-2026-58381
Red Hat--Red Hat Hardened Images	A flaw was found in the libblkid library of util-linux. During nested partition probing, the BSD, Minix, Solaris x86, and UnixWare partition probers cache a raw pointer to a parent partition entry in a dynamically allocated array. When subsequent partition additions cause the array to be reallocated, this pointer becomes stale, leading to a heap use-after-free read. An attacker who can present a crafted block device image (for example, via USB insertion or a loop-mounted disk image) can trigger this flaw without user interaction, as libblkid is invoked automatically by udev/udisks as root on block-device hot-plug events. This could lead to limited information disclosure or denial of service.	2026-06-29	6.8	CVE-2026-13595
Red Hat--Red Hat Satellite 6	A flaw has been found in foreman when HTTP parameters are modified in http_proxies_controller and http_proxy files. Attackers can perform an SSRF attack and steal cloud metadata service on AWS/GCP/Azure environment through foreman component.	2026-06-30	4.4	CVE-2026-13316
Red Hat--Red Hat Satellite 6.16 for RHEL 8	A flaw was found in Foreman. This broken access control vulnerability allows an authenticated user with host-edit permissions to retarget an existing lookup value override to a different host. This is achieved by modifying the match field through nested host attributes, effectively bypassing authorisation checks. The consequence is the potential for unauthorised modification of managed host configurations across different organisational and location boundaries.	2026-07-01	6.5	CVE-2026-5135
Red Hat--Red Hat Satellite 6.16 for RHEL 8	A flaw was found in foreman. Authenticated users with 'view_keypairs' permission can bypass taxonomy scoping, allowing them to download private SSH (Secure Shell) keys from other organizations by directly querying key pair IDs. This vulnerability leads to cross-tenant data exposure in multi-tenant deployments, potentially compromising sensitive information.	2026-07-01	6.5	CVE-2026-5142
Red Hat--Red Hat Satellite 6.16 for RHEL 8	A flaw was found in Foreman. An authenticated user with host-edit permissions could exploit a cross-tenant information disclosure vulnerability. This flaw occurs because the taxonomy_scope controller method does not properly validate organization and location IDs from nested request parameters, bypassing existing authorization checks. This allows the user to leak sensitive infrastructure metadata, including subnet	2026-07-01	4.3	CVE-2026-5138

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	topology, IP ranges, gateways, DNS servers, and VLAN IDs, from organizations and locations they are not authorized to access.			
rilwis--Slim SEO A Fast & Automated SEO Plugin For WordPress	The Slim SEO - A Fast & Automated SEO Plugin For WordPress plugin for WordPress is vulnerable to Unauthorized Private Content Disclosure in all versions up to, and including, 4.9.8 via the `/wp-json/slim-seo/meta-tags/ai` REST API endpoint. This is due to the endpoint's `permission_callback` performing only a top-level `edit_posts` capability check without verifying that the requesting user has read access to the specific post supplied via the `object.ID` parameter, allowing the `generate` function to pass the attacker-controlled post ID to `Data::get_post_content()`, which calls `get_post()` regardless of post status or ownership. This makes it possible for authenticated attackers with Contributor-level access and above to retrieve AI-generated summaries of the raw `post_content` of arbitrary posts they are not authorized to view - including private posts, drafts, pending, future, and password-protected content authored by other users - with the substance of the protected content disclosed via the HTTP response.	2026-07-01	4.3	CVE-2026-12408
rometheme--RTMKit	The RTMKit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Advanced Heading widget's 'Background Text' parameter in versions up to, and including, 2.0.7 This is due to insufficient output escaping on the 'background_text_heading' setting in the render() function, which concatenates the value directly into an HTML attribute without applying esc_attr(). This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-03	6.4	CVE-2026-8351
rometheme--RTMKit	The RTMKit (rometheme-for-elementor) plugin for WordPress is vulnerable to Local File Inclusion in versions up to, and including, 2.0.7 This is due to insufficient path validation on the 'template' parameter in the render_templates AJAX endpoint, which is used directly in a require/include statement without sanitization. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute files on the server ending in _templates.php, allowing the execution of any PHP code in those files.	2026-07-03	4.3	CVE-2026-5137
RT-Thread--RT-Thread	A weakness has been identified in RT-Thread up to 5.0.2. This affects the function sys_getaddrinfo of the file components/lwp/lwp_syscall.c. Executing a manipulation of the argument ai_addr can lead to memory corruption. The attack can only be executed locally. The exploit has been made available to the public and could be used for attacks. The pull request to fix this issue awaits acceptance.	2026-07-03	5.5	CVE-2026-14607
RT-Thread--RT-Thread	A flaw has been found in RT-Thread up to 5.2.2. Affected is the function read/write/sys_ioctl of the file components/lwp/lwp_syscall.c of the component Parameter Handler. Executing a manipulation can lead to divide by zero. The attack may be launched remotely. The exploit has been published and may be used. The pull request to fix this issue awaits acceptance.	2026-07-04	4.3	CVE-2026-14629
Samsung Open Source--Escargot	Time-of-check time-of-use (TOCTOU) race condition vulnerability in Samsung Open Source Escargot allows Leveraging Race Conditions. This issue affects Escargot: bab3a5797557014ce3c2e28419a6310cfba90d0d.	2026-06-30	5.9	CVE-2026-14160

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
SaturdayDrive-- Ninja Forms - File Uploads	The Ninja Forms - File Uploads plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.3.29. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to read all plugin debug log entries stored in the wp_nf3_log table or permanently delete all rows from that table.	2026-07-03	5.3	CVE-2026-12557
seladb-- PcapPlusPlus	A vulnerability was determined in seladb PcapPlusPlus 25.05. The impacted element is the function pcpp::SSLClientHelloMessage::getHandshakeVersion of the file Packet++/src/SSLHandshake.cpp of the component TLS Hello Handler. Executing a manipulation of the argument handshakeVersion can lead to heap-based buffer overflow. It is possible to launch the attack remotely. This attack is characterized by high complexity. The exploitability is regarded as difficult. The exploit has been publicly disclosed and may be utilized. This patch is called 98e671010bc7c87b95898c22ae289220ae92542b. It is best practice to apply a patch to resolve this issue.	2026-06-29	5.6	CVE-2026-13588
seladb-- PcapPlusPlus	A vulnerability was identified in seladb PcapPlusPlus 25.05. This affects the function pcpp::TelnetLayer::getSubCommand of the file Packet++/src/TelnetLayer.cpp of the component Telnet Subnegotiation Packet Handler. The manipulation leads to heap-based buffer overflow. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitability is reported as difficult. The exploit is publicly available and might be used. The identifier of the patch is 98e671010bc7c87b95898c22ae289220ae92542b. It is recommended to apply a patch to fix this issue.	2026-06-29	5.6	CVE-2026-13589
seladb-- PcapPlusPlus	A security flaw has been discovered in seladb PcapPlusPlus 25.05. This impacts the function pcpp::ModbusLayer::getLength in the library Packet++/header/ModbusLayer.h of the component Modbus Protocol Handler. The manipulation of the argument length results in heap-based buffer overflow. The attack can be launched remotely. A high complexity level is associated with this attack. The exploitability is said to be difficult. The exploit has been released to the public and may be used for attacks. The patch is identified as 4c90c3e3418a2b09dc82b7ca5775e9c1e22fe454. Applying a patch is advised to resolve this issue.	2026-06-29	5.6	CVE-2026-13590
Sendcloud-- Sendcloud Shipping	Missing Authorization vulnerability in Sendcloud Sendcloud Shipping allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Sendcloud Shipping: from n/a through 1.0.29.	2026-07-02	5.3	CVE-2026-57760
shohei.tanaka-- Japanized For WooCommerce	Unauthenticated Broken Access Control in Japanized For WooCommerce <= 2.9.12 versions.	2026-06-29	6.5	CVE-2026-57340
ShortPixel-- Enable Media Replace	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ShortPixel Enable Media Replace allows Stored XSS. This issue affects Enable Media Replace: from n/a through 4.2.1.	2026-07-01	5.9	CVE-2026-57722
ShortPixel-- ShortPixel Adaptive Images	Subscriber Cross Site Scripting (XSS) in ShortPixel Adaptive Images <= 3.11.3 versions.	2026-07-02	6.5	CVE-2026-57342

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Siemens--Mendix Studio Pro 10.11	A vulnerability has been identified in Mendix Studio Pro 10.11 (All versions), Mendix Studio Pro 10.12 (All versions), Mendix Studio Pro 10.13 (All versions), Mendix Studio Pro 10.14 (All versions), Mendix Studio Pro 10.15 (All versions), Mendix Studio Pro 10.16 (All versions), Mendix Studio Pro 10.17 (All versions), Mendix Studio Pro 10.18 (All versions), Mendix Studio Pro 10.19 (All versions), Mendix Studio Pro 10.20 (All versions), Mendix Studio Pro 10.21 (All versions), Mendix Studio Pro 10.22 (All versions), Mendix Studio Pro 10.23 (All versions), Mendix Studio Pro 10.24 (All versions < V10.24.21), Mendix Studio Pro 11.0 (All versions), Mendix Studio Pro 11.1 (All versions), Mendix Studio Pro 11.10 (All versions), Mendix Studio Pro 11.11 (All versions), Mendix Studio Pro 11.2 (All versions), Mendix Studio Pro 11.3 (All versions), Mendix Studio Pro 11.4 (All versions), Mendix Studio Pro 11.5 (All versions), Mendix Studio Pro 11.6 (All versions < V11.6.7), Mendix Studio Pro 11.7 (All versions), Mendix Studio Pro 11.8 (All versions), Mendix Studio Pro 11.9 (All versions). Affected versions of Mendix Studio Pro do not properly validate or sanitize project files processed during the build pipeline. This could allow an attacker who tricks a user into opening and running a specially crafted malicious project locally on their system to execute arbitrary code in the context of that user.	2026-06-30	5.4	CVE-2026-48192
SigNoz--signoz	SigNoz through 0.130.1 contains a broken access control vulnerability that allows authenticated users to access other organizations' alert rules by supplying a target rule UUID, as the alert rule store predicates fail to filter by organization ID. Attackers can read, edit, and delete alert rules belonging to other organizations by exploiting the missing tenant isolation check, bypassing multi-tenant access controls.	2026-06-29	6.4	CVE-2026-57956
silverstripe--silverstripe-framework	Silverstripe Framework is a PHP framework which powers the Silverstripe CMS. In versions prior to 6.2.2, the "Insert media from web" functionality in the CMS is vulnerable to XSS from a specially crafted embed. This issue was fixed in version 6.2.2/	2026-07-01	5.4	CVE-2026-54720
smub--WPForms AI Form Builder for WordPress Contact Forms, Payment Forms, Survey Form, Quiz & More	The WPForms - Easy Form Builder for WordPress - Contact Forms, Payment Forms, Surveys, & More plugin for WordPress is vulnerable to Improper Neutralization of CRLF Sequences ('CRLF Injection') in all versions up to, and including, 1.10.2 This is due to `get_reply_to_address()` processing the Reply-To display name through smart-tag expansion with context "notification" instead of "notification-reply-to", which bypasses email-address validation while `wpforms_sanitize_textarea_field()` intentionally preserves CR/LF characters that are never stripped before the display name is concatenated into the raw `Reply-To:` mail header string. This makes it possible for unauthenticated attackers to inject arbitrary additional email headers - such as `Bcc:` - into outgoing notification emails, silently blind-copying all notification email copies to an attacker-controlled address. Exploitation requires that a form notification is configured to use a Paragraph Text (textarea) field as the Reply-To display name via a Smart Tag.	2026-07-01	5.3	CVE-2026-12127
Snowflake--Snowflake CLI	Improper restriction of file path resolution in Snowflake CLI versions prior to 3.19 allowed arbitrary local file content to be read and transmitted to Snowflake services. An attacker could exploit this by supplying crafted repository or project content that referenced files outside the intended project boundary, causing Snowflake CLI to read local files and upload or embed their contents during deployment or SQL template processing.	2026-06-29	6.3	CVE-2026-13748

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Successful exploitation required the victim to process attacker-controlled project content, and retrieval of exfiltrated data depended on access to the victim's Snowflake account artifacts such as query history or uploaded stage content. The fix is available in Snowflake CLI version 3.19, and users must manually upgrade.			
Snowflake-- Snowflake CLI	Improper neutralization of parameters in Snowflake CLI versions prior to 3.19 allowed unintended SQL execution. An attacker could exploit this by supplying crafted values to vulnerable command paths, causing Snowflake CLI to execute unintended SQL in the context of the user's Snowflake session. Successful exploitation required crafted values to reach vulnerable parameters, including through socially engineered input, malicious repository configuration, or compromised automation feeding external values into the CLI, and impact is limited by the privileges assigned to the active session. The fix is available in Snowflake CLI version 3.19, and users must manually upgrade.	2026-06-29	6	CVE-2026-13752
Snowflake-- Snowflake CLI	Insertion of sensitive information into log files in Snowflake CLI versions prior to 3.19 allowed plaintext credentials to be written to persistent local debug logs. An attacker could exploit this by obtaining read access to the affected user's local log files, causing credentials such as passwords, tokens, or private key material to be exposed without additional application-level safeguards. Successful exploitation requires credentials to be present in the affected connection context and the resulting logs to be accessible from the local environment. The fix is available in Snowflake CLI version 3.19, and users must manually upgrade.	2026-06-29	5.5	CVE-2026-13750
Snowflake-- Snowflake CLI	Improper handling of untrusted remote references in Snowflake CLI versions prior to 3.19 allowed server-side request forgery. The SQL statement reader's !source/!load directives could reference remote URLs that were retrieved at runtime without sufficient restriction on the request destination. By supplying crafted SQL content processed through a vulnerable command path, an attacker could cause the victim's environment to issue unintended outbound requests to internal or otherwise non-public network locations, and could cause remote SQL content to be retrieved and executed in the context of the victim user's session. Successful exploitation requires the victim to process attacker-controlled content through a vulnerable command path and is limited by the privileges available to that session and environment. The fix is available in Snowflake CLI version 3.19, which adds an option to disable remote URL retrieval.	2026-06-29	4.1	CVE-2026-13751
Softaculous-- FormLayer	Insertion of Sensitive Information Into Sent Data vulnerability in Softaculous FormLayer allows Retrieve Embedded Sensitive Data. This issue affects FormLayer: from n/a through 1.0.6.	2026-07-05	5.3	CVE-2026-59519
SolarWinds-- Database Performance Analyzer	SolarWinds Database Performance Analyzer was found to be affected by a stored cross-site scripting vulnerability, which when exploited, can lead to unintended script execution.	2026-06-30	5.6	CVE-2026-28322
SourceCodester-- CET Automated Grading System with AI	A vulnerability was detected in SourceCodester CET Automated Grading System with AI Predictive Analytics 1.0. This issue affects some unknown processing. The manipulation results in session fixation. The attack can be executed remotely. The attack requires a high level of complexity. The	2026-07-03	5.6	CVE-2026-14609

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Predictive Analytics	exploitability is assessed as difficult. The exploit is now public and may be used.			
SourceCodester--CET Automated Grading System with AI Predictive Analytics	A security vulnerability has been detected in SourceCodester CET Automated Grading System with AI Predictive Analytics 1.0. This vulnerability affects unknown code of the file /index.php?action=view_student of the component POST Handler. The manipulation of the argument ID leads to authorization bypass. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used.	2026-07-03	4.3	CVE-2026-14608
SourceCodester--Multi-Vendor Online Grocery Management System	A security vulnerability has been detected in SourceCodester Multi-Vendor Online Grocery Management System 1.0. This impacts the function update_settings_info of the file classes/SystemSettings.php of the component Setting Handler. Such manipulation of the argument content[] leads to code injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used.	2026-07-05	6.3	CVE-2026-14691
SourceCodester--Multi-Vendor Online Grocery Management System	A vulnerability was detected in SourceCodester Multi-Vendor Online Grocery Management System 1.0/5.7.26. Affected is the function save_shop_type of the file classes/Master.php of the component POST Parameter Handler. Performing a manipulation results in sql injection. The attack is possible to be carried out remotely. The exploit is now public and may be used.	2026-07-05	6.3	CVE-2026-14692
SourceCodester--Multi-Vendor Online Grocery Management System	A vulnerability has been found in SourceCodester Multi-Vendor Online Grocery Management System 1.0. Affected by this issue is the function cancel_order of the file classes/Master.php of the component POST Parameter Handler. The manipulation of the argument ID leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2026-07-05	6.3	CVE-2026-14694
SourceCodester--Multi-Vendor Online Grocery Management System	A flaw has been found in SourceCodester Multi-Vendor Online Grocery Management System 1.0. Affected by this vulnerability is the function cancel_order of the file classes/Master.php. Executing a manipulation can lead to improper authorization. The attack may be performed from remote. The exploit has been published and may be used.	2026-07-05	5.4	CVE-2026-14693
SourceCodester--Online Boat Reservation System	A vulnerability was identified in SourceCodester Online Boat Reservation System 1.0. Affected by this vulnerability is an unknown functionality. Such manipulation leads to session expiration. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	2026-07-05	6.3	CVE-2026-14725
SourceCodester--Online Examination & Learning Management System	A vulnerability was identified in SourceCodester Online Examination & Learning Management System 1.0. Affected is an unknown function of the file /process_lesson.php. Such manipulation of the argument user_id leads to unrestricted upload. The attack may be launched remotely. The exploit is publicly available and might be used. The name of the affected product appears to have a typo in it.	2026-07-05	6.3	CVE-2026-14775
SourceCodester--Online Examination & Learning	A security flaw has been discovered in SourceCodester Online Examination & Learning Management System 1.0. Affected by this vulnerability is the function pathinfo of the file /upload_files.php of the component Filename Extension. Performing a manipulation results in unrestricted upload. Remote exploitation of the attack is possible. The exploit has been	2026-07-05	6.3	CVE-2026-14776

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	released to the public and may be used for attacks. The name of the affected product appears to have a typo in it.			
SourceCodester--Online Examination & Learning Management System	A weakness has been identified in SourceCodester Online Examination & Learning Management System 1.0. Affected by this issue is some unknown functionality of the file /announcements.php. Executing a manipulation can lead to unrestricted upload. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. The name of the affected product appears to have a typo in it.	2026-07-05	6.3	CVE-2026-14777
SourceCodester--Simple Food Ordering System	A flaw has been found in SourceCodester Simple Food Ordering System 1.0. The affected element is an unknown function of the file /cart.php. Executing a manipulation of the argument item_price can lead to business logic errors. The attack may be performed from remote. The exploit has been published and may be used.	2026-06-29	5.3	CVE-2026-13571
SourceCodester--Syllabus-Aligned Learning Management and Examination System	A security flaw has been discovered in SourceCodester Syllabus-Aligned Learning Management and Examination System 1.0. Impacted is an unknown function of the file upload_files.php. Performing a manipulation results in unrestricted upload. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks.	2026-07-05	6.3	CVE-2026-14698
spacetime--Ad Inserter Ad Manager & AdSense Ads	The Ad Inserter - Ad Manager & AdSense Ads plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to and including 2.8.16 via the 'data' attribute of the [adinsserter] shortcode. This is due to the replace_ai_tags() function processing a {reusable-block-N} tag pattern that calls get_post_field('post_content', N) without verifying the requesting user's capability with current_user_can('read_post'), without restricting the post type to 'wp_block', and without checking the post status. This makes it possible for authenticated attackers, with Contributor-level access and above, to read the full content of arbitrary posts including Private, Draft, Pending, Trashed, and password-protected posts owned by other users, by placing the shortcode in a post they own and previewing it.	2026-07-03	4.3	CVE-2026-11900
stellarwp--GiveWP Donation Plugin and Fundraising Platform	The GiveWP - Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'block_id' (and other) shortcode attributes of the 'givewp_campaign_comments' shortcode in versions up to, and including, 4.16.0. This is due to insufficient input sanitization and output escaping on user supplied attributes in CampaignCommentsShortcode::parseAttributes() and BlockRenderController::render(), where the blockId value is interpolated directly into a single-quoted HTML attribute without esc_attr(). This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-01	6.4	CVE-2026-13246
stellarwp--GiveWP Donation Plugin and Fundraising Platform	The GiveWP - Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'sequoia[introduction][image]' parameter in all versions up to, and including, 4.16.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Give Worker-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-02	6.4	CVE-2026-13704

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stellarwp-- GiveWP Donation Plugin and Fundraising Platform	The GiveWP plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 4.15.3 This is due to missing nonce validation on the give_set_notification_status_handler() function. This makes it possible for unauthenticated attackers to disable donation email notifications via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	2026-07-01	4.3	CVE-2026-11981
stellarwp-- Kadence Blocks Page Builder Toolkit for Gutenberg Editor	The Kadence Blocks - Page Builder Toolkit for Gutenberg Editor plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 3.7.7. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with contributor-level access and above, to create arbitrary Media Library attachments by downloading remote images to the site's uploads directory via wp_upload_bits() and wp_insert_attachment(), bypassing the upload_files capability boundary.	2026-07-01	4.3	CVE-2026-12902
stellarwp-- Kadence Blocks Page Builder Toolkit for Gutenberg Editor	The Kadence Blocks - Gutenberg Blocks for Page Builder Features plugin for WordPress is vulnerable to Insecure Direct Object Reference in versions up to and including 3.7.7. This is due to a mismatch between the object used for authorization and the object actually accessed in the Optimize_Rest_Controller's create_item(), get_item(), delete_item(), and bulk_delete_items() endpoints - authorization is checked via current_user_can('edit_post'/'delete_post', \$post_id) against the user-supplied post_id, while the storage layer keys analysis records on sha256(\$post_path) from a separately supplied, attacker-controlled post_path parameter, with no enforcement that post_path corresponds to post_id. This makes it possible for authenticated attackers, with Contributor-level access and above, to read or delete optimizer analysis records belonging to posts owned by other users by submitting their own post_id (which passes the capability check) together with the victim post's path.	2026-07-01	4.3	CVE-2026-12904
stephen-kruger-- bluebox	A vulnerability was found in stephen-kruger bluebox up to 4.5.12. Affected by this vulnerability is an unknown functionality. Performing a manipulation of the argument code results in cross site scripting. It is possible to initiate the attack remotely. The exploit has been made public and could be used. The project was informed of the problem early through an issue report.	2026-07-05	4.3	CVE-2026-14704
stephenharris-- Event Organiser	The Event Organiser plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 3.12.9. This is due to the 'eo_events' shortcode accepting attacker-controlled 'no_events' content and rendering it in event list templates without output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-01	6.4	CVE-2026-2387
StoneFly-- Storage Concentrator	Storage Concentrator (SC & SCVM) is vulnerable to reflected cross-site scripting due to unsanitized content being echoed back in 404 error pages. An attacker can craft a malicious URL that, when visited by an authenticated user, causes arbitrary script content to execute within the victim's browser session in the context of the application. This could be leveraged to steal session cookies, redirect users, or perform unauthorized actions on behalf of the victim.	2026-06-30	6.1	CVE-2026-50040

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Stormshield--Stormshield Network Security	A vulnerability was discovered on Stormshield Network Security 4.3.0 to 4.3.41 (included), 4.4.0 to 4.8.15 (included) , 5.0.2 EA to 5.0.5 (included) A revoked client certificate can still be used to authenticate to the captive-admin portal, allowing an attacker who possesses the revoked certificate to gain administrative access.	2026-07-01	4.3	CVE-2026-8480
Stormshield--Stormshield Network Security	A vulnerability was discovered on StormShield Network Security 4.3.0 to 4.3.41 (included), 4.8.0 to 4.8.15 (included) , 5.0.0 to 5.0.5 (included) There is a possible leak of secret information if administration commands have been passed with the CLI command line tool. Someone with SSH access to the firewall (if SSH multiuser mode is enabled) could possibly get the proxy CA passphrase or TPM password.	2026-07-02	4.3	CVE-2026-8482
strapi--strapi	Strapi users-permissions plugin fails to restrict JWT algorithms when plugin::users-permissions.jwt.algorithm is not explicitly configured, allowing acceptance of HS384 and HS512 tokens alongside HS256. Attackers possessing the jwtSecret can mint tokens with non-standard HMAC variants to bypass algorithm restrictions and weaken authentication controls.	2026-06-29	4.8	CVE-2026-57997
Strategy11 Team--Business Directory	Unauthenticated Cross Site Scripting (XSS) in Business Directory <= 6.4.22 versions.	2026-06-29	6.5	CVE-2026-57326
Strategy11 Team--Business Directory	Subscriber Cross Site Scripting (XSS) in Business Directory <= 6.4.22 versions.	2026-06-29	6.5	CVE-2026-57328
Strategy11 Team--Business Directory	Unauthenticated Broken Access Control in Business Directory <= 6.4.23 versions.	2026-06-29	6.6	CVE-2026-57339
Stylemix--MasterStudy LMS	Subscriber Cross Site Scripting (XSS) in MasterStudy LMS <= 3.7.27 versions.	2026-06-29	6.5	CVE-2026-57330
stylemix--Motors Car Dealership & Classified Listings Plugin	The Motors - Car Dealership & Classified Listings Plugin plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 1.4.111. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for authenticated attackers, with subscriber-level access and above, to mark or unmark any other user's car listing as sold by replaying a valid nonce harvested from their own listing against an arbitrary victim post ID, triggering a site-wide 'Sold' badge on the victim's listing and silently stripping its special_car featured post meta as a side effect. Exploitation requires the attacker to hold an active listing of their own (obtainable by a Subscriber via the plugin's add-listing form) in order to harvest a valid nonce for the 'stm_mark_as_sold_car' action, which can then be replayed against any other listing's post ID.	2026-07-01	4.3	CVE-2026-12435
StylemixThemes--Motors	Unauthenticated Broken Access Control in Motors <= 5.6.80 versions.	2026-07-02	6.5	CVE-2026-27433
Surbma--Surbma Yoast SEO	Contributor Cross Site Scripting (XSS) in Surbma Yoast SEO Breadcrumb Shortcode <= 1.2 versions.	2026-07-02	6.5	CVE-2026-57764

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Breadcrumb Shortcode				
taiga--taiga-back	Taiga before 6.10.2 contains a missing authorization vulnerability that allows unauthenticated remote attackers to create default due-date records in any project by exploiting unprotected POST endpoints on the user-story, task, and issue due-date API viewsets. Attackers can supply an arbitrary project identifier to these endpoints, which bypass permission checks and apply the AllowAny default, to pre-empt project administrators from initializing due dates by creating records before they can do so themselves.	2026-07-02	5.3	CVE-2026-59097
taskbuilder--Taskbuilder Project Management & Task Management Tool With Kanban Board	The Taskbuilder - Project Management & Task Management Tool With Kanban Board plugin for WordPress is vulnerable to generic SQL Injection via the 'wppm_proj_filter' parameter in all versions up to, and including, 5.0.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. No nonce verification is performed on the wp_ajax_wppm_view_project_tasks handler, meaning any authenticated session - including subscriber-level - can reach the vulnerable code path without any additional preconditions.	2026-07-01	6.5	CVE-2026-12090
taskbuilder--Taskbuilder Project Management & Task Management Tool With Kanban Board	The Taskbuilder - Project Management & Task Management Tool With Kanban Board plugin for WordPress is vulnerable to generic SQL Injection via the 'task_search' parameter in all versions up to, and including, 5.0.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. The wppm_get_task_list AJAX handler performs no capability check and no nonce verification, meaning any authenticated user including those with Subscriber-level access can invoke it directly.	2026-07-01	6.5	CVE-2026-12110
teableio--teable	Teable before 2026-06-15T04:43:24Z.1912 contains an improper access control vulnerability that allows anonymous attackers to access hidden field data by supplying arbitrary field IDs in the projection parameter of the share view records endpoint. Attackers can enumerate hidden field IDs from share metadata and specify them in projection parameters to read field values that are intended to be restricted from public view.	2026-06-29	5.3	CVE-2026-56781
themegrill--Zakra	The Zakra theme for WordPress is vulnerable to Stored Cross-Site Scripting via post meta values in all versions up to, and including, 4.2.0. This is due to the theme registering three post meta fields (zakra_menu_item_color, zakra_menu_item_hover_color, and zakra_menu_item_active_color) with 'show_in_rest' => true and 'auth_callback' => '__return_true', but without any sanitize_callback parameter in the register_post_meta() calls. While the classic editor save path applies sanitize_hex_color() sanitization, the REST API path completely bypasses this protection. The unsanitized meta values are then retrieved via get_post_meta() and concatenated directly into CSS strings that are output through wp_add_inline_style() without any escaping. This makes it possible for authenticated attackers, with	2026-07-03	6.4	CVE-2026-4804

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the injected page.			
themeisle--RSS Aggregator by Feedzy Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator	The RSS Aggregator by Feedzy - Feed to Post, Autoblogging, News & YouTube Video Feeds Aggregator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'aspectRatio' Attribute in all versions up to, and including, 5.2.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-02	6.4	CVE-2026-13252
ThemeREX--Booked	Unauthenticated Cross Site Request Forgery (CSRF) in Booked <= 3.0.0 versions.	2026-07-02	6.5	CVE-2026-57747
Themeum--Kirki	Unauthenticated Insecure Direct Object References (IDOR) in Kirki <= 6.0.11 versions.	2026-07-02	6.5	CVE-2026-57680
themeum--Kirki Freeform Page Builder, Website Builder & Customizer	The Kirki - Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 6.0.11 via the get_single_symbol. This makes it possible for unauthenticated attackers to extract the full builder metadata and rendered HTML of any kirki_symbol post - including unpublished drafts - by supplying a sequential WordPress post ID.	2026-07-02	5.3	CVE-2026-12122
themeum--Kirki Freeform Page Builder, Website Builder & Customizer	The Kirki - Freeform Page Builder, Website Builder & Customizer plugin for WordPress is vulnerable to authorization bypass in all versions up to, and including, 6.0.11. This is due to the plugin not properly verifying that a user is authorized to perform an action. This makes it possible for unauthenticated attackers to send arbitrary HTML-injected emails - including phishing messages embedding a real, valid WordPress password-reset URL for the targeted user - to any registered user via the site's own mail server, abusing its SPF/DKIM reputation. The attacker-controlled emailSubject parameter is passed to wp_mail() with only sanitize_text_field() applied, while emailBody 'text' items are concatenated raw into the HTML email body with no escaping, and 'chip' items can include the genuine WordPress password-reset link for the targeted account.	2026-07-02	5.3	CVE-2026-12472
themeum--Tutor LMS eLearning and online course solution	The Tutor LMS - eLearning and online course solution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Lesson Attachment Title in all versions up to, and including, 3.9.13 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-01	6.4	CVE-2026-13443
thimpress--LearnPress WordPress LMS Plugin for Create and Sell Online Courses	The LearnPress - WordPress LMS Plugin for Create and Sell Online Courses plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 4.3.9.1 via the 'userId' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to view the course enrollment progress and completion data belonging to any instructor or administrator account on the site. This IDOR does not apply when the target user is a regular subscriber, as the guard correctly blocks	2026-07-01	6.5	CVE-2026-11988

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	cross-subscriber access; exploitation is limited to cases where the victim user holds the LP_TEACHER_ROLE or administrator role.			
thimpress-- LearnPress WordPress LMS Plugin for Create and Sell Online Courses	The LearnPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'class_wrapper_form' shortcode attribute in versions up to, and including, 4.4.0. This is due to insufficient input sanitization and output escaping in the FilterCourseTemplate::sections() method at line 98, where the attacker-controlled attribute is inserted into an HTML class attribute via sprintf('<form class="%s">', \$class_wrapper_form) without esc_attr() escaping. The FilterCourseShortcode::render() handler does not apply shortcode_atts() filtering, so raw user attributes flow directly through do_action('learn-press/filter-courses/layout', \$data) into the template. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-01	6.4	CVE-2026-12732
Tim Strifler-- Exclusive Addons Elementor	Insertion of Sensitive Information Into Sent Data vulnerability in Tim Strifler Exclusive Addons Elementor allows Retrieve Embedded Sensitive Data. This issue affects Exclusive Addons Elementor: from n/a through 2.7.9.9.	2026-07-05	5.3	CVE-2026-59511
TR7 Cyber Defense Inc.-- WAF-ASP	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in TR7 Cyber-Defense Inc. WAF-ASP allows Stored XSS. This issue affects WAF-ASP: from v1.0.324.900 before v1.4.0.117.	2026-07-02	5.4	CVE-2026-4772
TR7 Cyber Defense Inc.-- WAF-ASP	Improper neutralization of input during web page generation ('cross-site scripting') vulnerability in TR7 Cyber-Defense Inc. Web Application Firewall allows DOM-Based XSS. This issue affects Web Application Firewall: from v1.0.42.239 before v1.4.0.117.	2026-07-02	4.6	CVE-2026-4770
trainingbusiness pros-- Groundhogg CRM, Newsletters, and Marketing Automation	The Groundhogg - CRM, Newsletters, and Marketing Automation plugin for WordPress is vulnerable to generic SQL Injection via the 'select' parameter in all versions up to, and including, 4.5.8 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with custom-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Exploitation requires the attacker to hold a Groundhogg custom role with the view_contacts capability, which is granted by default to several built-in Groundhogg roles above the base subscriber level.	2026-07-02	6.5	CVE-2026-14029
tranmautritam-- TheFox	Contributor Cross Site Scripting (XSS) in TheFox <= 3.9.70 versions.	2026-07-02	6.5	CVE-2026-57684
ultimatemember-- Ultimate Member User Profile, Registration, Login, Member Directory, Content Restriction &	The Ultimate Member - User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'about_me' parameter in all versions up to, and including, 2.11.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-03	6.4	CVE-2026-8489

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Membership Plugin				
uvnc--UltraVNC	UltraVNC repeater through 1.8.2.2 contains an integer overflow in the HTTP request logging path. In repeater/webgui/settings.c:336, the win_log() function allocates list nodes via malloc(sizeof(struct LIST) + strlen(line)), where line is derived from HTTP request URIs. If strlen(line) is sufficiently large, the addition overflows to a value smaller than sizeof(struct LIST), causing a heap allocation smaller than required. The subsequent strcpy of the full string into the undersized allocation produces a heap buffer overflow. In the current implementation this overflow is bounded by the HTTP receive buffer size (WI_RXBUFSIZE = 153600 bytes, well below SIZE_MAX on 32-bit builds), limiting practical exploitability to a partial heap write. A remote unauthenticated attacker can trigger the theoretical overflow path by sending a maximally-sized URI in an HTTP request to the repeater HTTP port.	2026-07-01	5.3	CVE-2026-7828
uvnc--UltraVNC	UltraVNC through 1.8.2.2 uses a cryptographically weak pseudo-random number generator to produce VNC authentication challenge bytes. In rfb/vncauth.c:119-129, the vncRandomBytes() function seeds libc rand() with time(0) + getpid() + rand() and generates a 16-byte challenge. The combined seed space is approximately 31 bits (libc rand() internal state) and is entirely determined by publicly-observable values (wall-clock time and process ID). An attacker who can observe the authentication exchange can enumerate the seed space and predict the challenge within seconds, enabling forgery or offline brute-forcing of responses. Note: on Windows, the active code path may use vncEncryptBytes2.cpp which calls CryptGenRandom; reachability on shipped Windows binaries requires compile-graph verification and is under investigation.	2026-07-01	4.8	CVE-2026-44040
uvnc--UltraVNC	UltraVNC through 1.8.2.2 contains an out-of-bounds read in the wide-string to multibyte conversion helper. In rfb/dh.cpp:204, the vncWc2Mb() function passes a caller-supplied WCHAR pointer to wcslen() before any bounds check. If the caller provides a wide-character buffer that is not properly NUL-terminated, wcslen() reads past the end of the buffer until it encounters a NUL wchar, resulting in an out-of-bounds read. Under typical Win32 API usage this requires an abnormal caller contract. Impact is limited to a potential information disclosure from adjacent memory regions or a process crash (denial of service) if the over-read crosses a page boundary.	2026-07-01	4.3	CVE-2026-44041
UX-themes--Flatsome	Contributor Broken Access Control in Flatsome <= 3.20.5 versions.	2026-07-02	6.5	CVE-2026-57731
UX-themes--Flatsome	Subscriber Broken Access Control in Flatsome <= 3.20.5 versions.	2026-07-02	4.3	CVE-2026-57730
VillaTheme--ALD Dropshipping and Fulfillment for AliExpress and WooCommerce	Unauthenticated Broken Authentication in ALD - Dropshipping and Fulfillment for AliExpress and WooCommerce <= 2.2.0 versions.	2026-07-02	4.8	CVE-2026-57352

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
villatheme--CURCY Multi Currency for WooCommerce Smoothly on WooCommerce 9.x	The The CURCY - Multi Currency for WooCommerce - Smoothly on WooCommerce 9.x plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.2.14. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	2026-07-03	5.4	CVE-2026-11778
vjinfotech--WP Import Export Lite	The WP Import Export Lite plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to and including 3.9.30 via the wpie_import_upload_file_from_url AJAX action. The plugin's URL downloader first calls wp_safe_remote_get() (which correctly blocks private/reserved IP ranges), but when that call returns a WP_Error - the exact outcome for any blocked internal host - the Download::download_file() method falls back to GuzzleHttp\Client::request() with the original attacker-supplied URL and no SSRF protection (and with TLS verification disabled). This makes it possible for authenticated attackers, with administrator-level access and above, to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services such as the cloud metadata endpoint at 169.	2026-07-03	5.5	CVE-2026-11397
Vsourz Digital--Advanced Contact form 7 DB	Subscriber Broken Access Control in Advanced Contact form 7 DB <= 2.0.9 versions.	2026-07-02	6.5	CVE-2026-57669
w1.fi--hostapd	In hostapd before 2.12, a missing bounds check in AP-mode Wi-Fi 7 (IEEE 802.11be) Multi-Link Operation (MLO) association request processing allows an unauthenticated attacker within wireless range to send a crafted management frame containing a malformed Multi-Link Element or Per-STA Profile subelement. In hostapd_process_ml_assoc_req() in src/ap/ieee802_11_ah.c, the received link_id field can be parsed as value 15, but the corresponding links[] storage only has valid entries for lower link IDs (0 through 14). This causes an out-of-bounds write / small memory corruption during association processing before the 4-way handshake. The attack does not require network credentials, prior authentication, or user interaction. The confirmed practical impact is denial of service through hostapd process termination. This affects hostapd v2.11 and newer development snapshots before v2.12 when built with CONFIG_IEEE80211BE enabled. The issue is fixed in hostapd v2.12 and the upstream 2026-1 fixes.	2026-06-30	6.5	CVE-2026-58374
wagtail--wagtail	Wagtail is an open source content management system built on Django. In versions prior to 7.0.8, 7.3.3 and 7.4.2, due to a missing permission check on the image preview endpoint, a user with access to the Wagtail admin can preview any image. The existing data of the image object itself is not exposed. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. This issue has been fixed in versions 7.0.8, 7.3.3, and 7.4.2.	2026-07-01	6.5	CVE-2026-54261
wagtail--wagtail	Wagtail is an open source content management system built on Django. In versions prior to 7.0.8, 7.3.3 and 7.4.2, the Documents and Images chooser's chosen endpoint incorrectly listed items for which the user has not been granted choose permission. A user with access to the Wagtail	2026-07-01	4.3	CVE-2026-54259

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	admin could see the filename and name and URLs of documents and images in those collections. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. This issue has been fixed in versions 7.0.8, 7.3.3, and 7.4.2.			
wagtail--wagtail	Wagtail is an open source content management system built on Django. In versions prior to 7.0.8, 7.3.3 and 7.4.2, an authenticated admin user can trigger expensive rendition processing with purposefully crafted filter specs resulting in potentially service degradation. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. This issue has been fixed in versions 7.0.8, 7.3.3, and 7.4.2.	2026-07-01	4.3	CVE-2026-54260
wagtail--wagtail	Wagtail is an open source content management system built on Django. In versions prior to 7.0.8, 7.3.3 and 7.4.2, a low-level user with the "Can submit translation" permission can create translations for any page, including those they do not have permissions for. This issue has been fixed in versions 7.0.8, 7.3.3, and 7.4.2.	2026-07-01	4.3	CVE-2026-54262
wappointment--Appointment Bookings for Zoom GoogleMeet and more Wappointment	The Appointment Bookings for Zoom GoogleMeet and more - Wappointment plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to and including 2.7.6 via the `appointmentkey` parameter due to the appointment `edit_key` - the sole authorization token consumed by `tryCancel()` - being generated as a predictable, unsalted MD5 hash of only `client_id` (a sequential integer), `start_at` (a publicly observable appointment timestamp), and `staff_id` (a small enumerable integer), with no secret salt or random component, and the unauthenticated cancellation and rescheduling REST endpoints performing no ownership or identity verification beyond matching this reconstructible key. This makes it possible for unauthenticated attackers to compute valid `edit_key` values for appointments belonging to other users and cancel or reschedule those appointments arbitrarily. Exploitation requires the `allow_cancellation` or `allow_rescheduling` setting to be enabled on the site, both of which are common configurations for active booking deployments; an attacker can obtain the inputs needed to reconstruct a victim's key by booking their own appointment to observe their sequential `client_id` and correlating publicly visible appointment times and enumerable staff identifiers.	2026-07-02	5.3	CVE-2026-9188
Wavlink--WL-NU516U1-A	A vulnerability was determined in Wavlink WL-NU516U1-A M16U1_V240425. The affected element is the function sub_401D68 of the file /cgi-bin/wireless.cgi of the component POST Parameter Handler. This manipulation of the argument SSID2G2/SSID5G2/AuthMethod2/WPAPSK12 causes command injection. Remote exploitation of the attack is possible. The exploit has been publicly disclosed and may be utilized. The affected component should be upgraded. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	2026-06-29	6.3	CVE-2026-13538
Webba Plugins--Webba Booking	Missing Authorization vulnerability in Webba Plugins Webba Booking allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Webba Booking: from n/a through 6.4.13.	2026-07-01	5.3	CVE-2026-27409

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
webpack-dev-server--webpack-dev-server	webpack-dev-server versions 5.2.5 and earlier terminate the whole Node.js process when an unauthenticated peer sends either a normal HTTP request with a malformed Host header or a WebSocket upgrade to the default /ws endpoint with a malformed Origin header. The malformed value causes an uncaught exception in the host-validation path and crashes the dev server. Impact is limited to availability of the development server, no data disclosure, no code execution. Patches: upgrade to webpack-dev-server 5.2.6. Workarounds: keep the dev server bound to localhost (the default) and do not expose it to untrusted networks.	2026-07-03	5.3	CVE-2026-14631
webpack-dev-server--webpack-dev-server	webpack-dev-server versions 5.2.5 and earlier expose two internal developer endpoints, /webpack-dev-server/open-editor and /webpack-dev-server/invalidate, that perform state-changing actions on any GET request without verifying that the request originated from the dev server's own page. Any website a developer visits while the dev server is running can trigger these endpoints cross-origin with no interaction beyond the visit. An attacker can open an arbitrary existing local file in the developer's editor, including files outside the project root, and repeated requests can spawn editor processes and force recompilations that degrade the developer's machine. Patches: upgrade to webpack-dev-server 5.2.6. Workarounds: none.	2026-07-03	4.7	CVE-2026-14620
wedevs--weDocs: AI Powered Knowledge Base, Docs, Documentation, Wiki & AI Chatbot	The weDocs: AI Powered Knowledge Base, Docs, Documentation, Wiki & AI Chatbot plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'sectionTitleTag' and 'articleTitleTag' Block Attributes in all versions up to, and including, 2.3.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-03	6.4	CVE-2026-12731
wedevs--weDocs: AI Powered Knowledge Base, Docs, Documentation, Wiki & AI Chatbot	The weDocs: AI Powered Knowledge Base, Docs, Documentation, Wiki & AI Chatbot plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'connectorWidth' Block Attribute in all versions up to, and including, 2.3.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-03	6.4	CVE-2026-12734
wedevs--weDocs: AI Powered Knowledge Base, Docs, Documentation, Wiki & AI Chatbot	The weDocs: AI Powered Knowledge Base, Docs, Documentation, Wiki & AI Chatbot plugin for WordPress is vulnerable to Missing Authorization in versions up to and including 2.3.0. This is due to a missing capability check on the do_migration() function registered as the wedocs_migrate_betterdocs_to_wedocs AJAX action, which performs no nonce verification via check_ajax_referer() and no capability check via current_user_can() before executing sensitive operations. This makes it possible for authenticated attackers, with Subscriber-level access and above, to trigger a full BetterDocs-to-weDocs data migration, creating and modifying 'docs' custom post type entries with attacker-controlled titles, updating site options, and deactivating the BetterDocs and BetterDocs Pro plugins via deactivate_plugins().	2026-07-03	4.3	CVE-2026-12729

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
weDevs--WP User Frontend	Unauthenticated Broken Access Control in WP User Frontend <= 4.3.7 versions.	2026-06-29	6.5	CVE-2026-57334
weng-xianhu--EyouCMS	A security vulnerability has been detected in weng-xianhu EyouCMS up to 1.7.1. This issue affects some unknown processing of the file /index.php of the component API. Such manipulation of the argument click_like leads to sql injection. The attack can be executed remotely. The exploit has been disclosed publicly and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-29	4.7	CVE-2026-13569
WofficeIO--Woffice	Missing Authorization vulnerability in WofficeIO Woffice allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects Woffice: from n/a before 5.4.33.	2026-07-01	5.3	CVE-2026-27435
WOOCOMMERCE DESIGNER PRO--WooCommerce Designer Pro	Subscriber Cross Site Scripting (XSS) in WooCommerce Designer Pro <= 1.9.34 versions.	2026-06-29	6.5	CVE-2026-57329
woodpecker-ci--woodpecker	Woodpecker before 3.15.0 registers the /api/orgs/lookup/*org_full_name endpoint without authentication middleware, and the LookupOrg handler unconditionally dereferences the session user (user.ForgeID, via ForgeFromUser) when selecting the forge to query. For an unauthenticated request session.User returns nil, so any unauthenticated HTTP request triggers a NULL pointer dereference in the handler. The panic is recovered by gin recovery middleware and the server continues serving (returning HTTP 500), but each request writes a multi-line panic stack trace to the error log. A low-bandwidth unauthenticated attacker can repeatedly probe the endpoint to flood the logs (about 37 lines per request), inflating disk usage and downstream log-ingestion cost and burying legitimate log events.	2026-06-30	5.3	CVE-2026-58369
WP Reloaded--ApplyOnline	Missing Authorization vulnerability in WP Reloaded ApplyOnline allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects ApplyOnline: from n/a through 2.6.7.6.	2026-07-01	5.3	CVE-2026-57721
wpchill--Kali Forms Contact Form & Drag-and-Drop Builder	The Kali Forms - Contact Form & Drag-and-Drop Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'meta[kaliforms_field_components]' parameter in all versions up to, and including, 2.4.13 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	2026-07-01	6.4	CVE-2026-9107
wplegalpages--Cookie Banner for GDPR / CCPA WPLP Cookie Consent	The Cookie Banner for GDPR / CCPA - WPLP Cookie Consent plugin for WordPress is vulnerable to generic SQL Injection via the 's' parameter in all versions up to, and including, 4.3.5 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	2026-07-03	4.9	CVE-2026-12920

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wpmart--Team Members Multi Language Supported Team Plugin	The Team Members - Multi Language Supported Team Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 8.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	2026-06-30	4.4	CVE-2026-12114
wpqode--Editorial Rating Product Review & Rating System	The Editorial Rating - Product Review & Rating System plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'Link URL' Field in all versions up to, and including, 4.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The WordPress unfiltered_html capability exemption does not apply here because the payload is stored in post meta (_wpas_er_options via update_post_meta) rather than in post_content or post_excerpt, meaning the restriction affects all administrators regardless of their unfiltered_html status.	2026-06-30	4.4	CVE-2026-12560
WSO2--WSO2 API Manager	The silent Just-In-Time (JIT) provisioning feature in federated authentication implementations fails to properly segregate user roles during account creation when a federated user shares a username with a local user. This allows the provisioning process to overwrite existing roles of local users with roles assigned to the federated user. Exploitation requires a federated identity provider (IDP) with silent JIT provisioning enabled and an attacker's knowledge of a local user's username. When these conditions are met, a malicious individual can leverage the JIT provisioning process to modify the roles of local users. The overwritten roles are limited to those defined within the federated IDP, typically granting minimal access rights unless explicitly configured otherwise by the federated IDP administrator.	2026-07-04	4.8	CVE-2024-1248
yahoo--elide	Elide through 7.1.17 fails to enforce @ReadPermission on client-supplied sort expressions in SortingImpl.getValidSortingRules, allowing attackers to sort collections by forbidden fields. Attackers can infer hidden field values through row ordering analysis, leaking relative field ordering across all rows via both JSON:API and GraphQL read paths.	2026-06-29	4.3	CVE-2026-57954
Yunai--ruoyi-vue-pro	ruoyi-vue-pro through 2026.05, fixed in commit c779a47, contains a missing authorization vulnerability in the CRM module's GET /admin-api/crm/follow-up-record/get endpoint that allows authenticated users to read any follow-up record by iterating sequential numeric IDs. Attackers can exploit this by sending requests with arbitrary ID parameters to access other users' follow-up notes, file attachments, scheduling information, and business entity references without proper authorization checks.	2026-06-29	6.5	CVE-2026-57949
YunaiV--yudao-cloud	yudao-cloud before 2026.06 contains a broken access control vulnerability in the BPM module that allows any authenticated user to access arbitrary process instance records by supplying a caller-controlled process-instance identifier to an unprotected endpoint lacking the @PreAuthorize annotation. Attackers can query any process-instance identifier through the unguarded GET endpoint to read sensitive workflow data including submitted form variables, approver identities, approval and rejection	2026-06-30	6.5	CVE-2026-58448

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	comments, and process BPMN XML without ownership or tenant party verification.			
YzmCMS-- YzmCMS	A vulnerability was determined in YzmCMS up to 7.5. This affects an unknown function of the file /application/install/index.php. Executing a manipulation of the argument siteurl can lead to sql injection. The attack can be executed remotely. A high complexity level is associated with this attack. The exploitability is reported as difficult. The exploit has been publicly disclosed and may be utilized. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-29	5.6	CVE-2026-13529
zephyrproject-- zephyr	mcumgr_serial_process_frag() in subsys/mgmt/mcumgr/transport/src/serial_util.c calls net_buf_reset() on the result of smp_packet_alloc() before checking it for NULL. smp_packet_alloc() uses net_buf_alloc(K_NO_WAIT) against the shared MCumgr packet pool (CONFIG_MCUMGR_TRANSPORT_NETBUF_COUNT, default 4), which returns NULL when the pool is exhausted. In default builds the __ASSERT_NO_MSG in net_buf_reset is a no-op, so net_buf_simple_reset writes through the NULL pointer (buf->len = 0; buf->data = buf->__buf), causing a fault/crash. The fragment data reaches this code from attacker-controlled bytes on the MCumgr serial/UART/shell-console transports (smp_uart.c, smp_raw_uart.c, smp_shell.c), and a fresh buffer is allocated at the start of essentially every new packet. An attacker on the serial/console link can flood the transport to drive the 4-entry buffer pool to exhaustion and induce the NULL dereference, crashing the device (denial of service). The defect was introduced after the original MCumgr rework and shipped in Zephyr v4.4.0. The fix moves the NULL check ahead of net_buf_reset.	2026-06-29	6.2	CVE-2026-10648
zephyrproject-- zephyr	The Zephyr net_buf library (lib/net_buf/buf.c) manipulated both of its reference counts -- the per-header buf->ref and the per-data-block ref_count at the start of each variable/heap data allocation -- with plain non-atomic C operators (buf->ref++, if (--buf->ref > 0), if (--(*ref_count))). The API is documented as self-synchronizing: callers may share one buffer across threads (e.g. via k_fifo) and each holder independently calls net_buf_unref() with no surrounding lock. Under true concurrency (SMP, or single-core preemption between the non-atomic load and store while another context unrefs the same buffer), two holders can both observe the same prior reference value and both conclude they are the last reference. For heap/variable-data pools (mem_pool_data_unref/heap_data_unref, used by zbus message subscribers, the IP stack RX/TX buffers when CONFIG_NET_BUF_FIXED_DATA_SIZE=n, capture, wireguard, ISO-TP and usbip) this produces a double k_heap_free()/k_free() of the same block -- heap-metadata corruption and a use-after-free on the heap-hardening poison pattern. For the per-header refcount the buffer is returned to the pool free LIFO twice for any pool type (including fixed-data pools used by Bluetooth and networking), corrupting the free list so a later allocation hands the same buffer to two owners. The fix converts both refcounts to atomic_inc/atomic_dec (overlying buf->ref in an atomic_t-sized union and changing the data-block refcount from uint8_t to atomic_t). Impact is gated on genuine concurrency and on an application architecture that shares one buffer among multiple independent unref'ers; the trigger is a refcount/timing race rather than packet content, so an external attacker	2026-06-30	6.4	CVE-2026-10653

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	has at most weak indirect influence over the race window. Affects all Zephyr releases through v4.4.0.			
zephyrproject--zephyr	The asynchronous SNTP client in Zephyr (subsys/net/lib/sntp/sntp.c, sntp_close_async) closed the UDP socket file descriptor directly from the calling thread immediately after detaching it from the network socket service, without synchronizing with the socket-service poll thread. The socket service thread polls each socket via zvfs_poll, which (in zsock_poll_prepare_ctx) registers a k_poll_event pointing into the socket's net_context (&ctx->recv_q) and then blocks in k_poll without holding a reference or lock. net_context objects are allocated from a fixed pool (contexts[CONFIG_NET_MAX_CONTEXTS]) and reused after close. When sntp_close_async is invoked from a different thread than the poll thread (in the in-tree consumer subsys/net/lib/config/init_clock_sntp.c, the SNTP timeout handler runs on the system workqueue while the socket service thread is blocked in poll on the same fd), the close frees and may reuse the net_context while the poll thread still has a poller node linked into the freed object, resulting in a use-after-free / object confusion of kernel poll structures. The SNTP timeout path is the normal no-response failure mode, so a network peer or off-path attacker who drops or delays the SNTP/NTP response can drive the racing close repeatedly (and periodically with NET_CONFIG_Sntp_INIT_RESYNC). The most likely consequence is a crash of the networking thread (denial of service), with potential memory corruption when the freed context slot is reallocated. The fix defers the close to the socket service thread itself via net_socket_service_close (NET_SOCKET_SERVICE_CLOSE_SOCKETS), so the same thread that polls performs the close, eliminating the race. Affected releases: v4.2.0 through v4.4.0.	2026-06-30	6.5	CVE-2026-10655
zephyrproject--zephyr	The Zephyr Bluetooth controller ISO Adaptation Layer (subsys/bluetooth/controller/ll_sw/isoal.c) fails to validate the length field of a framed ISO PDU start segment. Per the Bluetooth specification a start segment (sc=0) always carries a 3-byte time_offset, so its segment-header len must be at least PDU_ISO_SEG_TIMEOFFSET_SIZE (3). isoal_check_seg_header() accepted start segments with len < 3 as valid, and isoal_rx_framed_consume() then computed length = seg_hdr->len - 3 in a uint8_t, underflowing to 253-255 when len is 0-2. That oversized length is passed to isoal_rx_append_to_sdu(), whose copy is clamped only against the destination SDU buffer size, not the source PDU length, so up to ~255 bytes of controller memory beyond the received PDU are copied (via sink_sdu_write_hci()/net_buf_add_mem) into an HCI ISO data packet and delivered to the host. The PDU and its segment headers are entirely attacker-controlled and arrive over the air, reachable through both the CIS and BIS-sync HCI data paths (hci_driver.c) and the vendor data path (ull_iso.c), so a remote CIS peer or a broadcaster the device is synced to can trigger an out-of-bounds read causing information disclosure to the host and potential denial of service (faults or malformed oversized HCI ISO packets). The flaw affects all Zephyr releases since framed ISO reception was introduced in v3.0.0. The fix rejects sc=0 segments with len < 3 in isoal_check_seg_header() and adds a guard before the subtraction in isoal_rx_framed_consume().	2026-06-30	6.5	CVE-2026-9263
zephyrproject--zephyr	The USB CDC-NCM device class (subsys/usb/device_next/class/usbd_cdc_ncm.c) ignores the return value	2026-06-29	5.3	CVE-2026-10647

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	of <code>usb_ep_enqueue()</code> in its ethernet transmit callback <code>cdc_ncm_send()</code>. When the enqueue fails, the function still calls <code>k_sem_take(&data-sync_sem, K_FOREVER)</code>, blocking on a completion semaphore that is only ever signaled from the bulk-IN transfer-completion callback. Because nothing was enqueued, that callback never fires and the calling thread - a shared network traffic-class TX thread - deadlocks permanently while holding the interface TX lock, halting transmission until reboot (and leaking the transmit buffer). The enqueue fails under conditions controlled by the attached USB host: <code>usb_ep_enqueue()</code> returns <code>-EPERM</code> whenever the bus is suspended (a standard, persistent host operation), and the underlying <code>udc_ep_enqueue()</code> returns <code>-EPERM</code>/<code>-ENODEV</code> on disconnect, bus reset, or endpoint disable. The <code>cdc_ncm_send()</code> guard only checks the <code>DATA_IFACE_ENABLED</code> and <code>IFACE_UP</code> flags, not the suspended state, so a packet transmitted while the host holds the bus suspended reaches the failing enqueue and deadlocks the TX path. The realistic trigger is a bus suspend that occurs while the exported network interface is active and has traffic to send - host sleep, USB selective/auto-suspend, or hub power management - after which any device-originated packet deadlocks the path, recoverable only by reboot. The impact is a persistent loss of the virtual network connection between the host's NCM interface and the Zephyr device; because the deadlocked thread is a shared traffic-class TX thread, egress on other network interfaces can stall as well. There is no memory corruption or information disclosure. The defect was introduced with the CDC-NCM driver and shipped in releases through v4.4.0; it is fixed by checking the <code>usb_ep_enqueue()</code> return value and freeing the buffer before the blocking wait.			
zephyrproject--zephyr	Zephyr's DNS resolver (<code>subsys/net/lib/dns</code>) parses resource records from DNS responses in <code>dns_unpack_answer()</code>, which validated only the fixed RR header (type, class, TTL, rlength) and accepted any attacker-declared rlength, including one extending past the end of the received datagram. The TXT and SRV consumers in <code>dns_validate_record()</code> (<code>resolve.c</code>) then read up to rlength bytes (clamped only to a record-type maximum such as <code>DNS_MAX_TEXT_SIZE</code>, default 64, not to the packet) from the receive buffer via <code>memcpy</code> without their own bounds check, and pass the result to the application's resolve callback. A malicious or spoofed DNS server, an on-path attacker forging UDP DNS replies, or (with mDNS/LLMNR enabled) any LAN node can craft a truncated TXT or SRV response that causes an out-of-bounds read of adjacent receive-pool memory; the disclosed stale bytes (residual contents of prior DNS packets / uninitialized pool memory) are returned to the application as TXT/SRV record contents, an information leak, and may in some configurations cross the allocation boundary and fault, causing a denial of service. The read is bounded (~64 bytes for TXT, ~6 for SRV) and read-only (no write). The fix rejects any record whose declared rdata extends past <code>dns_msg->msg_size</code> at the single chokepoint in <code>dns_unpack_answer()</code>. Affected: v4.3.0 and v4.4.0.	2026-06-30	4.8	CVE-2026-10652
zephyrproject--zephyr	The MAX32xxx USB device controller driver (<code>drivers/usb/udc/udc_max32.c</code>, compatible <code>adi_max32_usbhs</code>) dereferenced an endpoint buffer in its OUT and IN transfer-completion handlers without checking it for NULL. <code>udc_event_xfer_out_done()</code> called <code>net_buf_add(buf, ep_request->actlen)</code> immediately after <code>buf = udc_buf_get(ep_cfg)</code>, where <code>udc_buf_get()</code> returns NULL when the endpoint FIFO is empty. A transfer-completion event is queued from	2026-07-05	4.6	CVE-2026-10656

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	interrupt context and processed asynchronously by the driver thread; between queuing and processing, the endpoint FIFO can be drained by host-controlled control flow - in particular udc_setup_received() drains the EPO OUT/IN FIFOs whenever a new SETUP packet arrives, and dequeue/disable/purge paths drain it likewise. A USB host that aborts an in-flight EPO control transfer with a new SETUP packet (legal USB behavior) can therefore cause a stale XFER_OUT_DONE event to be processed against an empty FIFO, producing net_buf_add(NULL, ...), a near-NULL pointer dereference that faults and crashes the device. No authentication is required; the attacker is the USB host the device is connected to (physical bus access). Impact is denial of service (device crash). The defect was introduced when the MAX32 UDC driver was added and shipped in Zephyr v4.4.0. The fix adds NULL-buffer checks that return early with UDC_EVT_ERROR/-ENOBUS in both the OUT-done and IN-done handlers.			
zhayujie-- chatgpt-on- wechat CowAgent	A weakness has been identified in zhayujie chatgpt-on-wechat CowAgent 2.1.0. This issue affects the function verify_server of the file channel/wechatmp/common.py of the component wx Endpoint. This manipulation of the argument wechatmp_token causes missing authentication. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. Upgrading to version 2.1.1 is capable of addressing this issue. Patch name: 3d7c68bac6ee74fad63f43cf99e45c62e202ed55. It is suggested to upgrade the affected component. The project confirms: "We've added an explicit non-empty check for wechatmp_token in verify_server() so that the /wx endpoint now fails closed with 403 Forbidden whenever the token is missing or left at the default empty value, instead of relying on a signature check that silently degenerates to a predictable hash."	2026-07-05	6.5	CVE-2026-14714
Zozothemes-- Corpkit	Subscriber Sensitive Data Exposure in Corpkit <= 1.0.5 versions.	2026-07-02	6.5	CVE-2025-69132

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1Panel-dev--CordysCRM	A security vulnerability has been detected in 1Panel-dev CordysCRM up to 1.4.1. This impacts the function Save of the file src/main/java/cn/cordys/crm/system/service/ModuleFormService.java of the component ModuleFormController. The manipulation of the argument Description leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed publicly and may be used. Upgrading to version 1.7.0 will fix this issue. The identifier of the patch is c87682afa8df79853299f75489c9d333f7bc5fce. Upgrading the affected component is recommended.	2026-06-02	3.5	CVE-2026-10567
1Panel-dev--CordysCRM	A vulnerability has been found in 1Panel-dev CordysCRM up to 1.6.2. This affects an unknown function of the file backend/framework/src/main/java/cn/cordys/config/RequestParamTrimC onfig.java. The manipulation leads to cross site scripting. Remote exploitation of the attack is possible. The exploit has been disclosed to the public and may be used. Upgrading to version 1.7.0 mitigates this issue. The identifier of the patch is c87682afa8df79853299f75489c9d333f7bc5fce. It is suggested to upgrade the affected component.	2026-06-01	2.4	CVE-2026-10514
Aiven-Open--klaw	Klaw is a self-service Apache Kafka Topic Management/Governance tool/portal. Prior to version 2.10.4, a vulnerability exists in the user registration and login mechanisms due to inconsistent handling of username case sensitivity, leading to a targeted Denial of Service (DoS) and complete account lockout. This issue has been patched in version 2.10.4.	2026-06-02	2.7	CVE-2026-44367
Assimp--Assimp	A security vulnerability has been detected in Assimp up to 6.0.4. Affected by this issue is the function HL1MDLLoader::read_sequence_infos of the file HL1MDLLoader.cpp of the component Half-Life 1 MDL Loader. The manipulation of the argument aiString leads to out-of-bounds read. The attack needs to be performed locally. The exploit has been disclosed publicly and may be used. The project tagged the reported issue as bug.	2026-06-01	3.3	CVE-2026-10233
bytedance--InfiniStore	A vulnerability was found in bytedance InfiniStore up to 0.2.33. The impacted element is the function purge_kv_map in the library /src/infinistore.h of the component KV Map Handler. Performing a manipulation results in inefficient algorithmic complexity. The attack requires a local approach. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-05	3.3	CVE-2026-11312
cilium--ebpf	A vulnerability has been found in cilium ebpf up to 0.21.0. This affects the function loadRawSpec of the file bt/btf.go of the component LoadCollectionSpec/LoadCollectionSpecFromReader. Such manipulation of the argument offset leads to integer overflow. The attack can only be performed from a local environment. The exploit has been disclosed to the public and may be used. The name of the patch is 533dfc82fd228bfadf42ea7180c39de7d9af47fa. A patch should be applied to remediate this issue.	2026-06-03	3.3	CVE-2026-10722
code-projects--Online Hospital	A weakness has been identified in code-projects Online Hospital Management System 1.0. This issue affects some unknown processing of the file viewdoctortimings.php. This manipulation of the argument delid causes improper control of resource identifiers. The attack can be initiated	2026-06-01	3.8	CVE-2026-10299

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Management System	remotely. The exploit has been made available to the public and could be used for attacks.			
dask--dask	A flaw has been found in dask up to 3.0. Affected by this issue is the function <code>nunique_approx</code> of the file <code>dask/dataframe/hyperloglog.py</code> of the component HLL Handler. This manipulation causes resource consumption. The attack is possible to be carried out remotely. A high degree of complexity is needed for the attack. The exploitation is known to be difficult. The pull request to fix this issue awaits acceptance.	2026-06-03	3.1	CVE-2026-10705
djangoproject--daphne	daphne before 4.2.2 reconstructs a raw HTTP request from Twisted's parsed headers and feeds it to autobahn for WebSocket handshake processing. Twisted does not treat <code>\x0b</code> , <code>\x0c</code> , <code>\x1c</code> , <code>\x1d</code> , <code>\x1e</code> , or <code>\x85</code> as header line separators, but autobahn decodes header values to str and calls <code>splitlines()</code> . An attacker can exploit this parser differential to inject additional headers into the ASGI scope passed to the application. daphne now rejects requests with these bytes in any header value with a 400 response.	2026-06-03	3.7	CVE-2026-44546
djangoproject--Django	An issue was discovered in Django 5.2 before 5.2.15 and 6.0 before 6.0.6. <code>`django.middleware.cache.UpdateCacheMiddleware`</code> in Django does not add <code>`Authorization`</code> to the <code>`Vary`</code> response header for requests bearing that header without <code>`Cache-Control: public`</code> , which allows remote attackers to read private cached responses via unauthenticated requests to the same URL. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Shai Berger for reporting this issue.	2026-06-03	3.1	CVE-2026-35193
djangoproject--Django	An issue was discovered in Django 5.2 before 5.2.15 and 6.0 before 6.0.6. <code>`django.utils.cache.has_vary_header()`</code> in Django does not strip leading or trailing whitespace from <code>`Vary`</code> response header values before comparison, which allows remote attackers to read cached responses via requests to URLs whose responses contain whitespace-padded Vary header values. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Navid Rezazadeh for reporting this issue.	2026-06-03	3.1	CVE-2026-48587
djangoproject--Django	An issue was discovered in Django 6.0 before 6.0.6 and 5.2 before 5.2.15. <code>`django.http.HttpRequest.get_signed_cookie`</code> in Django uses a non-injective salt derivation (concatenating the cookie name and salt argument), which allows a remote attacker to use a cookie in a context different from the one where it was signed, via distinct <code>`(name, salt)`</code> pairs that produce the same concatenation. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Peng Zhou for reporting this issue.	2026-06-03	3.1	CVE-2026-6873
djangoproject--Django	An issue was discovered in Django 6.0 before 6.0.6 and 5.2 before 5.2.15. <code>`django.core.mail.backends.smtp.EmailBackend`</code> in Django fails to prevent reuse of a partially-initialized connection after a failed <code>`STARTTLS`</code> handshake when <code>`fail_silently=True`</code> , which allows on-path network attackers to read email content via cleartext interception. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Kasper Dupont for reporting this issue.	2026-06-03	3.1	CVE-2026-7666

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
django--Django	An issue was discovered in Django 5.2 before 5.2.15 and 6.0 before 6.0.6. `django.middleware.cache.UpdateCacheMiddleware` in Django does not match `Cache-Control` response directives case-insensitively, which allows remote attackers to read responses that were incorrectly cached because their `Cache-Control` directives used uppercase or mixed-case values. Earlier, unsupported Django series (such as 5.0.x, 4.1.x, and 3.2.x) were not evaluated and may also be affected. Django would like to thank Ahmed Badawe for reporting this issue.	2026-06-03	3.1	CVE-2026-8404
FluentCMS--FluentCMS	A weakness has been identified in FluentCMS 0.0.5. The impacted element is an unknown function of the file /admin/blocks of the component Blocks Plugin. This manipulation causes cross site scripting. The attack may be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-06	2.4	CVE-2026-11434
ggml-org--whisper.cpp	A security flaw has been discovered in ggml-org whisper.cpp up to 1.8.2. This vulnerability affects the function whisper_model_load of the file ggml/src/ggml.c. The manipulation results in null pointer dereference. Attacking locally is a requirement. The exploit has been released to the public and may be used for attacks. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	3.3	CVE-2026-10298
gradio-app--gradio	A security flaw has been discovered in gradio-app gradio 6.14.0. This affects the function save_audio_to_cache of the component Audio Cache Key Handler. Performing a manipulation results in use of weak hash. The attack must be initiated from a local position. The attack is considered to have high complexity. It is indicated that the exploitability is difficult. The exploit has been released to the public and may be used for attacks. The patch is named 13394. To fix this issue, it is recommended to deploy a patch.	2026-06-03	2.5	CVE-2026-10783
HCL--iControl	HCL iControl was affected by Missing Cookie Attributes vulnerability. It was observed that the application is missing several critical cookie attributes, including Secure and SameSite. And also path is set to root.	2026-06-04	3.1	CVE-2025-52608
HCL--iControl	HCL iControl was affected by Missing Security Headers vulnerability. which lead to cross-site scripting (XSS) attacks by enabling the built-in XSS filtering mechanisms of modern web browsers.	2026-06-04	3.7	CVE-2025-52609
HCL--iControl	HCL iControl v4.0.0 was affected by Unhandled Exception - Stack Trace Disclosure vulnerability. The error occurs due to an undefined property being accessed in the application's JavaScript code. Specifically, the code attempts to read the property dashboard key from an object that is undefined. This issue likely stems from one of the following: A missing or improperly initialized object.	2026-06-04	3.1	CVE-2025-52611
HCL--iReflection	HCL iReflection Third party vulnerable and outdated components issue was detected in the web application	2026-06-02	3.1	CVE-2024-42206
HCLSoftware--BigFix Cloud Lifecycle Management	HCL BigFix Cloud Lifecycle Management is affected by lack of input validation. This low-level flaw allows unauthorized access and may lead to information exposure.	2026-06-04	3.3	CVE-2025-62338

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
janet-lang--janet	A security flaw has been discovered in janet-lang janet up to 1.41.0. This affects the function doframe of the file src/core/debug.c. Performing a manipulation results in out-of-bounds read. Attacking locally is a requirement. The exploit has been released to the public and may be used for attacks. The patch is named ed17dd2c5913a23fb1107251e44a9410a3c30cf5.	2026-06-01	3.3	CVE-2026-10267
janet-lang--janet	A weakness has been identified in janet-lang janet up to 1.41.0. This vulnerability affects the function unmarshal_one_fiber of the file src/core/marsh.c. Executing a manipulation can lead to integer overflow. It is possible to launch the attack on the local host. The exploit has been made available to the public and could be used for attacks. This patch is called d9b1d711ea1fde52ac73a82088b512a3e17bad0d. A patch should be applied to remediate this issue.	2026-06-01	3.3	CVE-2026-10268
JeecgBoot--JeecgBoot	A vulnerability was identified in JeecgBoot up to 3.9.2. Affected by this vulnerability is the function queryPageList of the file src\main\java\org\jeecg\modules\system\controller\SysUserController.java of the component User List Endpoint. The manipulation of the argument salt leads to information disclosure. The attack may be initiated remotely. The attack is considered to have high complexity. The exploitation appears to be difficult. The exploit is publicly available and might be used. A fix is planned for the upcoming release.	2026-06-07	3.1	CVE-2026-11464
kiteworks--Secure Data Forms	Kiteworks is a private data network (PDN). Prior to version 9.3.0, an Insecure Direct Object Reference (IDOR) vulnerability in Kiteworks Secure Data Forms allows an authenticated user to access metadata of resources belonging to other users due to insufficient authorization checks on resource ownership. Upgrade Kiteworks to version 9.3.0 or later to receive a patch.	2026-06-01	3.7	CVE-2026-24761
lharries--whatsapp-mcp	A vulnerability was determined in lharries whatsapp-mcp 0.0.1. Affected by this vulnerability is the function SendMessageRequest of the file whatsapp-bridge/main.go of the component Send API Endpoint. This manipulation of the argument mediaPath causes path traversal. The exploit has been publicly disclosed and may be utilized. Patch name: 6657cdceadd361e8fbe824afe9d00b4504009a5d. It is recommended to apply a patch to fix this issue.	2026-06-01	3.5	CVE-2026-10264
LMCache--LMCache	A flaw has been found in LMCache up to 0.4.6. This affects the function hex_hash_to_int16 of the file lmcache/integration/vllm/utils.py of the component KV Cache Handler. Executing a manipulation can lead to use of weak hash. The attack needs to be launched locally. The attack requires a high level of complexity. It is indicated that the exploitability is difficult. The exploit has been published and may be used. The pull request to fix this issue awaits acceptance.	2026-06-04	3.6	CVE-2026-10813
mcmilk--7-Zip	7-Zip is a file archiver with a high compression ratio. Versions 9.11 through 26.00 contain a heap out-of-bounds read of up to 3 bytes in the UDF disc image handler's File Identifier Descriptor parser. In CFileId::Parse (CPP/7zip/Archive/Udf/UdfIn.cpp), after validating size < 38 + idLen + implen and advancing processed to 38 + implen + idLen, the alignment-padding loop reads p[processed] while incrementing up to 3 times to reach a 4-byte boundary, and the processed <= size bounds check only runs after the loop. When (38 + implen + idLen) % 4 != 0 and 38 + implen + idLen ==	2026-06-05	3.1	CVE-2026-48102

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	size, the loop reads 1 to 3 bytes past the end of the exact-size heap buffer allocated via buf.Alloc((size_t)item.Size). The UDF handler is registered for .iso and .udf files and auto-detected by signature, and the OOB read triggers during Open() when listing or extracting a crafted UDF image. Impact is limited to information disclosure (a 1-bit oracle per OOB byte via open/fail behavior) and denial of service (crash under hardened allocators); there is no write primitive. Version 26.01 fixes the issue.			
Mettle--sendportal	A vulnerability was detected in Mettle sendportal up to 3.0.1. This affects an unknown part of the file /webview/ of the component Campaign Handler. The manipulation of the argument content results in cross site scripting. The attack can be launched remotely. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	3.5	CVE-2026-10234
MLflow--MLflow	A flaw has been found in MLflow up to 3.10.0. This issue affects the function mlflow.data.digest_utils of the file mlflow/data/digest_utils.py of the component Dataset Digest Computation. This manipulation causes use of weak hash. It is possible to launch the attack on the local host. The attack is considered to have high complexity. The exploitability is assessed as difficult. The exploit has been published and may be used. The project was informed of the problem early through a pull request but has not reacted yet.	2026-06-04	3.6	CVE-2026-10803
mlrun--mlrun	A vulnerability has been found in mlrun up to 1.12.0-rc3. This impacts the function mlrun.utils.helpers.calculate_dataframe_hash of the file mlrun/utils/helpers.py of the component DataFrame Hash Handler. The manipulation leads to use of weak hash. The attack can only be performed from a local environment. The complexity of an attack is rather high. The exploitability is said to be difficult. The exploit has been disclosed to the public and may be used. The pull request to fix this issue awaits acceptance.	2026-06-03	3.6	CVE-2026-10766
modelscope--ms-swift	A security vulnerability has been detected in modelscope ms-swift up to 4.2.0. This affects the function Template._save_pil_image of the file swift/template/base.py of the component PIL Image Cache Key Handler. The manipulation leads to use of weak hash. An attack has to be approached locally. A high degree of complexity is needed for the attack. It is indicated that the exploitability is difficult. The exploit has been disclosed publicly and may be used. The pull request to fix this issue awaits acceptance.	2026-06-04	3.6	CVE-2026-10801
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. From versions 1.15.0 to before 1.15.4, 1.16.0 to before 1.16.3, 1.17.0 to before 1.17.1, and 1.18.0 to before 1.18.1, a malicious user with access to an end-to-end encrypted files drop link was able to also drop files into other end-to-end encrypted folders of the share owner. Reading and modifying of other files was not possible. This issue has been patched in versions 1.15.4, 1.16.3, 1.17.1, 1.18.1, and 2.0.0-rc.7.	2026-06-01	3.5	CVE-2026-45159
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. Prior to versions 21.1.10, 22.0.11, and 23.0.3, a low-privileged user can force other user's microphones to be muted in calls when no High-performance Backend is installed. This issue has been patched in versions 21.1.10, 22.0.11, and 23.0.3.	2026-06-01	3.5	CVE-2026-45266

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. Prior to version 2.7.2, authenticated users can check if arbitrary files are associated with specific approval workflows where they can request approval. This issue has been patched in version 2.7.2.	2026-06-01	3.3	CVE-2026-45277
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. From version 6.1.0 to before version 8.2.2, an attacker can craft links that would redirect users to another website, when the victim uses the attackers link to log in via user OIDC. This issue has been patched in version 8.2.2.	2026-06-01	3.3	CVE-2026-45278
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. From version 2.6.0 to before version 4.3.0, when a previous collective pages was deleted and the collective was shared view-only, guests with access to the collective were able to access the deleted pages directly from the trashbin. This issue has been patched in version 4.3.0.	2026-06-01	2.6	CVE-2026-45154
nextcloud--security-advisories	Nextcloud is an open source content collaboration platform. In Nextcloud Server from versions 32.0.0 to before 32.0.7 and 33.0.0 to before 33.0.1, a missing access check on API level allowed to add unknown circles by their ID directly to other circles. Since circle IDs have 62^15 complexity by default this is still unlikely to be executable at will, but if access to an ID was available via another source, memberships could be tracked like this. It is recommended that the Nextcloud Server is upgraded to 32.0.7 or 33.0.1. It is recommended that the Nextcloud Enterprise Server is upgraded to 29.0.16.14, 30.0.17.8, 31.0.14.3, 32.0.7 or 33.0.1	2026-06-01	2.6	CVE-2026-45155
onnx--onnx-mlir	A vulnerability has been found in onnx onnx-mlir up to 0.5.0.0. Affected by this issue is the function generate_hash_key of the file src/Runtime/python/torch_onnxmlir/src/torch_onnxmlir/backend.py of the component Placeholder Node Cache Handler. Such manipulation leads to use of weak hash. An attack has to be approached locally. A high complexity level is associated with this attack. The exploitation is known to be difficult. The name of the patch is 72c5187ff6d13c2c2b3d3789b8f5faf99f08a5b4. Applying a patch is advised to resolve this issue.	2026-06-05	3.6	CVE-2026-11329
open-telemetry--opentelemetry-ebpf-instrumentation	OpenTelemetry eBPF Instrumentation provides eBPF instrumentation based on the OpenTelemetry standard. Prior to version 0.9.0, the Java TLS ioctl probe reads user-controlled ioctl pointers with bpf_probe_read instead of bpf_probe_read_user. An instrumented local process can therefore point OBI at kernel memory and cause that memory to be copied into telemetry. This issue has been patched in version 0.9.0.	2026-06-02	3.8	CVE-2026-45683
Open5GS--Open5GS	A security flaw has been discovered in Open5GS up to 2.7.6. The impacted element is the function gmm_state_security_mode of the file src/amf/gmm-sm.c of the component NGAP Handover. Performing a manipulation results in race condition. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitability is regarded as difficult. The exploit has been released to the public and may be used for attacks. The pull request to fix this issue awaits acceptance.	2026-06-02	3.1	CVE-2026-10565
OpenStack--Neutron	In OpenStack Neutron before 28.0.1, a project manager can create or update a port on a shared network owned by another project and set device_owner to a value that has "network:" at the beginning ("network:dhcp" for example). The default port RBAC policies incorrectly included PROJECT_MANAGER without requiring network ownership,	2026-06-04	2.2	CVE-2026-50266

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allowing any project manager to obtain trusted network-service port behavior on shared networks. Depending on backend and deployment, this can bypass anti-spoofing and security group protections, enabling DHCP, MAC, or IP spoofing against other tenants on the shared network. This is a regression of CVE-2015-5240 (OSSA-2015-018).			
Orthanc--DICOM Server	A security flaw has been discovered in Orthanc DICOM Server up to 1.12.11. This issue affects the function DcmItem::read of the file OrthancFramework/Sources/DicomParsing/FromDcmtkBridge.cpp of the component DCMTK Parser. Performing a manipulation results in stack-based buffer overflow. Attacking locally is a requirement. The exploit has been released to the public and may be used for attacks. The patch is named bae99026ca97. To fix this issue, it is recommended to deploy a patch.	2026-06-02	3.3	CVE-2026-10528
OTRS AG--OTRS	An incorrect handling of permissions in OTRS External Interface and the ConfigItem List module allows an authenticated customer to query the system for CI information. Please note that CMDb has to be enabled and CustomerGroupSupport has to be used to be affected. This issue affects OTRS: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.4.X	2026-06-01	3.5	CVE-2026-48190
OTRS AG--OTRS	An incorrect handling of permissions in STORM powered by OTRS and in OTRS (2026.x and above) Document Search Article Meta Filters modules allows gaining knowledge about number of affected CIs, SLA and services without gaining access to them. This issue affects OTRS with STORM modules: * 7.0.X * 8.0.X * 2023.X * 2024.X * 2025.X * 2026.X before 2026.4.X	2026-06-01	3.5	CVE-2026-48191
PaddlePaddle--FastDeploy	A weakness has been identified in PaddlePaddle FastDeploy up to 2.4.1. Affected by this issue is the function hash_features of the file fastdeploy/multimodal/hashe.py of the component MultimodalHasher. Executing a manipulation can lead to use of weak hash. The attack requires local access. A high complexity level is associated with this attack. The exploitation is known to be difficult. This patch is called 374945747652a8d32965591c0c01a00c88b7067f. Applying a patch is advised to resolve this issue.	2026-06-04	3.6	CVE-2026-10800
projectcapsule--capsule	Capsule is a multi-tenancy and policy-based framework for Kubernetes. To defend against namespace hijacking achieved through update/patch operations on namespaces, Capsule uses a webhook to validate update requests targeting namespaces. However, in Kubernetes, the namespace/finalize and namespace/status subresource APIs can also modify various fields of a namespace, including the metadata field. Prior to version 0.13.0, the webhook does not define interception rules for these subresources. As a result, if a tenant administrator has permission to modify namespace/status or namespace/finalize, they can successfully perform namespace hijacking. Version 0.13.0 fixes the issue. Another mitigation is to add two subresources (namespaces and namespaces/status with namespace/finalize within it) to the resources list in the ValidatingWebhookConfiguration rules.	2026-06-01	3.9	CVE-2026-30963
raisulislamg4--student_management_system_by_php	A vulnerability was found in raisulislamg4 student_management_system_by_php up to 310d950e09013d5133c6b9210aff9444382d16d1. The impacted element is an unknown function of the file admission_form_check.php. The	2026-06-01	3.5	CVE-2026-10228

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	manipulation of the argument Message results in cross site scripting. The attack can be executed remotely. The exploit has been made public and could be used. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.			
Red Hat--Red Hat Build of Keycloak	A flaw was found in org.keycloak.services. An administrator with delegated access to read group memberships and users can bypass user profile permissions by accessing the group members endpoint. This allows the administrator to view user attributes that are explicitly configured to be denied, leading to information disclosure.	2026-06-05	2.7	CVE-2026-9088
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in gnutls. The PKCS#7 padding check, performed during decryption, was not constant-time. This timing side-channel could allow a remote attacker to potentially leak sensitive information about the padding bytes through observable timing differences. This vulnerability is a form of information disclosure.	2026-06-01	3.7	CVE-2026-5419
SecureAge--CatchPulse	A security vulnerability has been detected in SecureAge CatchPulse up to 10.9.1. Impacted is an unknown function in the library saappctl.sys of the component IOCTL Handler. The manipulation leads to information disclosure. Local access is required to approach this attack. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-07	3.3	CVE-2026-11459
sgl-project--SGLang	A vulnerability was determined in sgl-project SGLang up to 0.5.11. Affected by this vulnerability is the function data_hash of the component Cache Handler. This manipulation causes denial of service. The attack is restricted to local execution. A high degree of complexity is needed for the attack. The exploitation appears to be difficult. The exploit has been publicly disclosed and may be utilized. The pull request to fix this issue awaits acceptance.	2026-06-03	3.6	CVE-2026-10775
SGLang--SGLang	A security vulnerability has been detected in SGLang 0.5.10.post1. Impacted is an unknown function of the file python/sglang/srt/lora/lora_manager.py of the component Inference HTTP Endpoint. Such manipulation of the argument lora_path leads to reachable assertion. The attack can be launched remotely. A high complexity level is associated with this attack. The exploitability is considered difficult. The exploit has been disclosed publicly and may be used. The pull request to fix this issue awaits acceptance.	2026-06-01	3.7	CVE-2026-10300
songquanpeng--one-api	A security flaw has been discovered in songquanpeng one-api up to 0.6.11-preview.7. Affected by this issue is the function Redeem of the file model/redemption.go of the component Redemption Code Top-Up Endpoint. The manipulation results in business logic errors. The attack may be launched remotely. The attack requires a high level of complexity. The exploitation is known to be difficult. The exploit has been released to the public and may be used for attacks. The pull request to fix this issue awaits acceptance.	2026-06-07	3.1	CVE-2026-11465
SourceCodester--Customer Review App	A vulnerability was found in SourceCodester Customer Review App 1.0. Affected by this vulnerability is the function add_review/save_review/get_all_reviews of the file review_app.py. Performing a manipulation of the argument name/comment results in	2026-06-01	3.3	CVE-2026-10295

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	denial of service. The attack requires a local approach. The exploit has been made public and could be used.			
SourceCodester--Hospitals Patient Records Management System	A vulnerability was detected in SourceCodester Hospitals Patient Records Management System 1.0. This issue affects some unknown processing of the file /admin/?page=room_types. Performing a manipulation of the argument room results in cross site scripting. The attack is possible to be carried out remotely. The exploit is now public and may be used.	2026-06-07	2.4	CVE-2026-11468
SourceCodester--Pharmacy Sales and Inventory System	A vulnerability was detected in SourceCodester Pharmacy Sales and Inventory System 1.0. Affected by this vulnerability is the function create_medicine_name of the file /ShowForm/create_medicine_name/main. Performing a manipulation of the argument medicine_name results in cross site scripting. The attack can be initiated remotely. The exploit is now public and may be used.	2026-06-01	3.5	CVE-2026-10244
SourceCodester--Pharmacy Sales and Inventory System	A flaw has been found in SourceCodester Pharmacy Sales and Inventory System 1.0. Affected by this issue is the function create_supplier of the file /ShowForm/create_supplier/main. Executing a manipulation of the argument company_name can lead to cross site scripting. The attack can be launched remotely. The exploit has been published and may be used.	2026-06-01	3.5	CVE-2026-10245
SourceCodester--Pharmacy Sales and Inventory System	A vulnerability has been found in SourceCodester Pharmacy Sales and Inventory System 1.0. This affects the function create_medicine_presentation of the file /ShowForm/create_medicine_presentation/main. The manipulation of the argument medicine_presentation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2026-06-01	3.5	CVE-2026-10246
SourceCodester--Pharmacy Sales and Inventory System	A vulnerability was found in SourceCodester Pharmacy Sales and Inventory System 1.0. This vulnerability affects the function create_generic_name of the file /ShowForm/create_generic_name/main. The manipulation of the argument generic_name results in cross site scripting. The attack may be launched remotely. The exploit has been made public and could be used.	2026-06-01	3.5	CVE-2026-10247
SourceCodester--Ship Ferry Ticket Reservation System	A security vulnerability has been detected in SourceCodester Ship Ferry Ticket Reservation System 1.0. Impacted is an unknown function of the file /admin/?page=user/manage_user. The manipulation of the argument Username leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed publicly and may be used.	2026-06-05	2.4	CVE-2026-11338
Streamlit--Streamlit	A vulnerability has been found in Streamlit up to 1.53.0. Impacted is an unknown function in the library lib/streamlit/runtime/caching/hashing.py of the component Palette Handler. Such manipulation leads to use of weak hash. Local access is required to approach this attack. The attack requires a high level of complexity. The exploitability is considered difficult. The exploit has been disclosed to the public and may be used. The pull request to fix this issue awaits acceptance.	2026-06-04	3.6	CVE-2026-10804
strawberry-graphql--strawberry	Strawberry GraphQL is a library for creating GraphQL APIs. In versions 0.288.4 through 0.315.3, Strawberry's bundled GraphQL template wrote values from the GraphQL headers editor into the browser URL query string. If a user entered a sensitive header, such as `Authorization: Bearer <token>`, the value could become visible in browser history, copied links,	2026-06-04	3.1	CVE-2026-45739

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and server/proxy/CDN access logs after a page reload or shared request. Version 0.315.4 patches the issue.			
thetodmack-- claude-mem	A weakness has been identified in thetodmack claude-mem up to 11.0.1. The affected element is the function computeObservationContentHash of the file src/services/sqlite/observations/store.ts of the component Observation Content Hash Handler. This manipulation causes use of weak hash. The attack can only be executed locally. The attack's complexity is rated as high. The exploitability is described as difficult. Upgrading to version 12.0.0 is sufficient to fix this issue. Patch name: f32fda8b35e9fe9329f87da65c31149362a03f97. It is suggested to upgrade the affected component.	2026-06-05	3.6	CVE-2026-11330
unitedbyai-- droidclaw	A vulnerability was detected in unitedbyai droidclaw up to 0.5.3. The affected element is an unknown function of the file server/src/routes/pairing.ts of the component claim Endpoint. The manipulation results in improper restriction of excessive authentication attempts. The attack may be launched remotely. This attack is characterized by high complexity. The exploitability is described as difficult. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-01	3.7	CVE-2026-10216
westboy-- CicadasCMS	A weakness has been identified in westboy CicadasCMS up to 2431154dac8d0735e04f1fd2a3c3556668fc8dab. Impacted is an unknown function of the file src/main/java/com/zhiliao/module/web/system/ScheduleJobController.java of the component Task Scheduling Management Module. Executing a manipulation can lead to cross site scripting. The attack can be executed remotely. The exploit has been made available to the public and could be used for attacks. This product implements a rolling release for ongoing delivery, which means version information for affected or updated releases is unavailable. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-02	2.4	CVE-2026-10529
wpvividplugins-- WPvivid Backup, Migration & Staging	The Migration, Backup, Staging - WPvivid Backup & Migration plugin for WordPress is vulnerable to arbitrary directory deletion due to insufficient file path validation in the delete_cancel_staging_site() function in all versions up to, and including, 0.9.128. This makes it possible for authenticated attackers, with Administrator-level access and above, to delete arbitrary folders on the server, which leads to a loss of data.	2026-06-05	3.8	CVE-2025-12656
zilliztech-- GPTCache	A vulnerability was detected in zilliztech GPTCache up to 0.1.44. Affected by this issue is the function BufferedReader.peek of the file gptcache/processor/pre.py of the component Cache Key Handler. Performing a manipulation of the argument input_data["image"] results in use of weak hash. The attack must be initiated from a local position. The attack is considered to have high complexity. The exploitation is known to be difficult. The exploit is now public and may be used. The pull request to fix this issue awaits acceptance.	2026-06-04	3.6	CVE-2026-10812
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized write	2026-06-09	3.5	CVE-2026-48288

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	access. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page.			
Adobe--Adobe Experience Manager	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page.	2026-06-09	3.5	CVE-2026-48289
apostrophecms--apostrophe	ApostropheCMS is an open-source Node.js content management system. In versions up to and including 4.30.0, when `prettyUrls: true` is enabled on `@apostrophecms/file` (a documented SEO feature for serving uploaded files at clean URLs), the public pretty-URL handler builds the upstream URL using the raw `Host` HTTP request header. That URL is then `fetch`'ed and the response body + headers are streamed straight back to the requester. Because `Host` is fully attacker-controlled, an unauthenticated remote attacker can pivot the apostrophe process to issue outbound HTTP requests against any host it can reach on the private network. The path component is constrained to `/uploads/attachments/<cuid>-<slug>.<ext>` (built from a local-DB lookup), which keeps the impact narrow: cross-instance data exfiltration is neutralized by cuid uniqueness, but blind-SSRF residuals remain (network-topology mapping via response-code / timing differences and verbose proxy/WAF 404 body disclosure). As of time of publication, no known patched versions exist.	2026-06-12	3.7	CVE-2026-53607
axios--axios	Axios is a promise based HTTP client for the browser and Node.js. From 1.15.2 to before 1.16.0, nested objects created by utils.merge() (e.g., config.proxy) are still constructed as plain {} with Object.prototype in their chain. The setProxy() function at lib/adapters/http.js:209-223 reads proxy.username, proxy.password, and proxy.auth without hasOwnProperty checks. When Object.prototype.username is polluted, setProxy() constructs a Proxy-Authorization header with attacker-controlled credentials and injects it into every proxied HTTP request. This vulnerability is fixed in 1.16.0.	2026-06-11	3.7	CVE-2026-44489
Bolt--CMS	A weakness has been identified in Bolt CMS up to 3.7.5. This vulnerability affects unknown code of the file src/Storage/Field/Type/TextType.php of the component HTML Attribute Handler. Executing a manipulation of the argument style can lead to HTML injection. It is possible to launch the attack remotely. The exploit has been made available to the public and could be used for attacks. The GitHub repository was archived by the owner and is now read-only. This vulnerability only affects products that are no longer supported by the maintainer.	2026-06-08	3.5	CVE-2026-11511
CodeAstro--Human Resource Management System	A vulnerability was identified in CodeAstro Human Resource Management System 1.0. Affected by this issue is some unknown functionality of the file /dashboard/add_tod of the component Dashboard Interface. The manipulation of the argument todo_data leads to cross site scripting. The attack may be initiated remotely. The exploit is publicly available and might be used.	2026-06-12	3.5	CVE-2026-12129

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
CodeAstro--Human Resource Management System	A security flaw has been discovered in CodeAstro Human Resource Management System 1.0. This affects an unknown part of the file /Projects/Add_Projects of the component Projects Management Page. The manipulation of the argument protitle results in cross site scripting. The attack may be launched remotely. The exploit has been released to the public and may be used for attacks.	2026-06-12	3.5	CVE-2026-12130
CodeAstro--Human Resource Management System	A vulnerability was identified in CodeAstro Human Resource Management System 1.0. Impacted is an unknown function of the file /notice/All_notice of the component Notice Board Management. Such manipulation of the argument Notice Title with the input <svg onload="alert('Stored XSS Triggered by Ashik Mohamed')"> as part of POST leads to cross site scripting. It is possible to launch the attack remotely. The exploit is publicly available and might be used.	2026-06-08	2.4	CVE-2026-11491
D-Link--DGS-1100-08PD	A vulnerability was identified in D-Link DGS-1100-08PD 1.00.006. This issue affects some unknown processing of the file /etc/boa.conf of the component Web Interface. Such manipulation leads to least privilege violation. The attack may be launched remotely. The attack requires a high level of complexity. The exploitability is assessed as difficult. The exploit is publicly available and might be used.	2026-06-08	3.7	CVE-2026-11555
fission--fission	Fission is an open-source, Kubernetes-native serverless framework that simplifies the deployment of functions and applications on Kubernetes. Prior to version 1.25.0, SanitizeFilePath in pkg/utils/utils.go validated that a path stayed under a safe directory by calling strings.HasPrefix(path, safedir). This is a lexical check, not a directory boundary check: /packages-extra/evil starts with /packages, so it passed. The function did not enforce a path-separator boundary, so any sibling directory whose name began with the safe-directory string was accepted. Callers included the builder's Clean handler (pkg/builder/builder.go:208) and the fetcher's Fetch / Upload handlers (pkg/fetcher/fetcher.go). A tenant who could pre-create or control a sibling directory under the fetcher / builder's shared volume could induce a write or read outside the intended safe directory. This issue has been patched in version 1.25.0.	2026-06-10	3.6	CVE-2026-50568
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 12.0 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2 that under certain conditions could have allowed an authenticated user to access confidential issue details due to incorrect authorization checks.	2026-06-11	3.1	CVE-2026-3553
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.9 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2 that under certain conditions could have allowed an authenticated user with developer-role permissions to hide changes from merge request diff views due to improper input handling of file names.	2026-06-11	3.7	CVE-2026-6976
GitLab--GitLab	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 15.9 before 18.10.8, 18.11 before 18.11.5, and 19.0 before 19.0.2 that under certain conditions, could have allowed an unauthenticated user to impersonate the GitLab Support Bot and inject arbitrary content via a specially crafted Service Desk email reply due to improper neutralization in email template processing.	2026-06-11	2.6	CVE-2026-9694

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Groww--Stock, Mutual Fund, Gold App	A vulnerability was identified in Groww Stock, Mutual Fund, Gold App up to 20260805 on Android. This affects an unknown part of the component WebView URL Handler. The manipulation leads to improper authorization in handler for custom url scheme. It is possible to launch the attack on the physical device. The complexity of an attack is rather high. It is indicated that the exploitability is difficult. The exploit is publicly available and might be used. The vendor was contacted early about this disclosure.	2026-06-12	1.8	CVE-2026-12065
Huawei--HarmonyOS	Permission control vulnerability in service notifications. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	3.6	CVE-2026-41974
Huawei--HarmonyOS	Logic bypass vulnerability in the file system. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	2.4	CVE-2026-41986
imvks786--student_management_system	A vulnerability was detected in imvks786 student_management_system up to 9599b560ad3c3b83e75d328b76bedcd489ef1f46. Affected by this issue is some unknown functionality of the file /add.php. The manipulation of the argument name/address/fname results in cross site scripting. It is possible to launch the attack remotely. The exploit is now public and may be used. This product takes the approach of rolling releases to provide continuous delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-08	3.5	CVE-2026-11534
JeecgBoot--JeecgBoot	A weakness has been identified in JeecgBoot up to 3.9.2. Impacted is the function HttpServletResponse.sendRedirect of the file jeecg-module-system/jeecg-system-biz/src/main/java/org/jeecg/modules/system/controller/ThirdLoginController.java of the component Third-Party Login. This manipulation of the argument state causes open redirect. The attack can be initiated remotely. A high degree of complexity is needed for the attack. The exploitability is considered difficult. The exploit has been made available to the public and could be used for attacks. The project replied: "After evaluation, this vulnerability has low exploitability in real-world scenarios: 1) Exploiting this vulnerability requires attackers to use social engineering techniques to induce victims to actively click on an OAuth login link constructed by the attacker; it cannot be triggered passively. 2) Third-party login (DingTalk/WeChat, etc.) is an optional feature and may not be enabled in most projects."	2026-06-08	3.1	CVE-2026-11502
jelmer--dulwich	Dulwich is a pure-Python implementation of the Git file formats and protocols. Starting in version 0.24.0 and prior to version 1.2.5, dulwich.porcelain.format_patch(outdir=...) derives each patch filename from the commit's subject line. Prior to this fix, get_summary only replaced spaces with dashes - path separators (/ , \), parent-directory components (.), and other filename-hostile characters (e.g. :) were preserved verbatim and passed straight into os.path.join(outdir, f"{i:04d}-{summary}.patch"). A malicious commit subject could therefore direct the generated patch file outside the requested outdir. This is fixed in Dulwich 1.2.5. Users should upgrade to 1.2.5 or later. dulwich.patch.get_summary now mirrors git's format_sanitized_subject: only `[A-Za-z0-9._]` are kept, runs of other characters collapse to a single -, consecutive . collapse to a single ., trailing ./- are stripped, and the result is length-limited. This makes the returned string safe to embed as a filename component, so format_patch can no longer be steered out of outdir via the commit	2026-06-10	3.3	CVE-2026-47712

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	subject. Until upgrading, callers that pass untrusted commits to porcelain.format_patch can use stdout=True and write the patch to a destination they control, rather than letting format_patch choose the filename; validate the chosen path before opening - e.g. compare os.path.realpath(returned_path) against os.path.realpath(outdir) and reject any patch whose resolved path is not inside outdir; and/or pre-screen commits and refuse to format any whose subject's first line contains /, \, .., or other characters that are not safe on the target filesystem.			
kokke--tiny-regex-c	A flaw has been found in kokke tiny-regex-c up to f2632c6d9ed25272987471cdb8b70395c2460bdb. This vulnerability affects the function matchstar of the file re.c of the component Pattern Handler. This manipulation causes inefficient regular expression complexity. The attack is restricted to local execution. The exploit has been published and may be used. This product adopts a rolling release strategy to maintain continuous delivery. Therefore, version details for affected or updated releases cannot be specified. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-08	3.3	CVE-2026-11478
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information over a network.	2026-06-09	3.3	CVE-2026-45455
Microsoft--Microsoft 365 Apps for Enterprise	Protection mechanism failure in Microsoft Office Excel allows an unauthorized attacker to bypass a security feature locally.	2026-06-09	3.3	CVE-2026-45459
Microsoft--Microsoft 365 Apps for Enterprise	Heap-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-06-09	3.3	CVE-2026-45466
Microsoft--Microsoft 365 Apps for Enterprise	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-06-09	3.3	CVE-2026-45485
Microsoft--Windows 10 Version 1607	Improper input validation in Microsoft Azure Attestation service and Device Health Attestation Service allows an authorized attacker to perform spoofing with a physical attack.	2026-06-09	3.9	CVE-2026-45642
nationalsecurityagency--ghidra	Ghidra before 12.1 contains a path traversal vulnerability in SameDirDebugInfoProvider that fails to validate filenames from ELF binary .gnu_debuglink sections before constructing file paths. Attackers can craft malicious ELF binaries with traversal sequences to probe filesystem existence and leak CRC32 hashes of arbitrary files during automatic DWARF analysis.	2026-06-10	3.3	CVE-2026-49497
nationalsecurityagency--ghidra	Ghidra before 11.2 contains a use after free vulnerability in the Sleigh backend caused by undefined static initialization order of the SleighArchitecture::translators and XmlArchitectureCapability singletons. Attackers can trigger an infinite loop or denial of service during shutdown	2026-06-10	2.9	CVE-2024-58350

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	by exploiting the unsafe destruction order that causes iteration over deallocated memory.			
OpenClaw--OpenClaw	OpenClaw before 2026.4.25 contains a policy bypass vulnerability in embedded runner policy that allows requests using provider aliases to compare against aliases instead of canonical provider identities. Attackers can exploit this confusion to select bundled tool access outside intended provider policy restrictions when the affected feature is enabled.	2026-06-11	3.8	CVE-2026-53809
OpenClaw--OpenClaw	OpenClaw before 2026.5.6 contains an improper access control vulnerability in Mattermost event handlers that fails to validate channel type metadata. Attackers can bypass intended DM policy decisions by sending crafted Mattermost events missing channel type information to process restricted content.	2026-06-12	3.7	CVE-2026-53837
Red Hat--Red Hat Directory Server 11	A heap buffer overflow flaw was found in 389 Directory Server. When audit logging is enabled, the create_masked_entry_string() function in auditlog.c copies a fixed-length password mask into a precisely-sized heap buffer without checking available space. If a short cleartext password is logged (requiring non-default CLEAR password storage or a compromised replication peer), the copy overflows the buffer, corrupting heap memory and audit log output.	2026-06-09	3.3	CVE-2026-11792
Red Hat--Red Hat Directory Server 11	A flaw was found in 389 Directory Server. The LDIF parser reads past the end of a heap buffer when processing attribute types with trailing semicolons during database import, causing an out-of-bounds read detectable under memory instrumentation.	2026-06-09	1.9	CVE-2026-11786
rikyoz--bit7z	bit7z is a cross-platform C++ static library that allows the compression/extraction of archive files. Prior to version 4.0.12, a one-byte off-by-one error in SafeOutPathBuilder::restoreSymlink() allows an attacker to craft a .7z archive that, when extracted with bit7z on any non-Windows platform, creates a symlink escaping the intended output directory. Subsequent archive entries extracted through this symlink write arbitrary files outside the extraction directory with the permissions of the extracting process. This issue has been patched in version 4.0.12.	2026-06-10	3.6	CVE-2026-45380
SAP_SE--SAP Business Objects	Under certain conditions, when an unauthorized attacker accesses a specific endpoint, SAP Business Objects application leaks sensitive information .This has a low impact on the confidentiality of the data. There is no impact on integrity and availability of the application.	2026-06-09	3.7	CVE-2026-44743
shopware--shopware	Shopware is an open commerce platform. Prior to versions 6.6.10.18 and 6.7.10.1, an attacker is able to enumerate the usernames of administrator users by performing a timing attack. Versions 6.6.10.18 and 6.7.10.1 fix the issue.	2026-06-10	3.7	CVE-2026-48011
SourceCodester--Inventory System	A weakness has been identified in SourceCodester Inventory System 1.0. Affected by this issue is some unknown functionality of the file header.php. This manipulation causes cross site scripting. It is possible to initiate the attack remotely. The exploit has been made available to the public and could be used for attacks. Multiple parameters might be affected.	2026-06-08	3.5	CVE-2026-11520
Spring--Spring Framework	Applications may be vulnerable to a Regular Expression Denial of Service (ReDoS) attack if an attacker is able to provide a pattern which is then	2026-06-09	3.7	CVE-2026-41848

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	directly or indirectly supplied to one of the following methods in AntPathMatcher: match(String pattern, String path), matchStart(String pattern, String path), extractUriTemplateVariables(String pattern, String path). Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.			
Spring--Spring Framework	A vulnerability in Spring Expression Language (SpEL) evaluation logic allows for arbitrary zero-argument method invocation, even within restricted or read-only contexts, which may allow an attacker to invoke unintended application logic. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	3.7	CVE-2026-41852
Spring--Spring Security	Since Spring Security SAML decrypts SAML Responses as well as elements of SAML LogoutRequests and LogoutResponses without requiring a valid signature, attackers may be able to craft these SAML payloads and use the Service Provider as a decryption oracle. Affected versions: Spring Security 5.7.0 through 5.7.23; 5.8.0 through 5.8.25; 6.3.0 through 6.3.16; 6.4.0 through 6.4.16; 6.5.0 through 6.5.10; 7.0.0 through 7.0.5.	2026-06-09	3.7	CVE-2026-41694
Spring--Spring Web Services	Wss4jSecurityInterceptor did not consistently wire Apache WSS4J ReplayCache instances into RequestData for validation-time checks. As a result, protections against replay of UsernameToken nonces and creation timestamps, Timestamp elements, and certain SAML one-time-use semantics could be ineffective even when operators configured a replay cache on the interceptor. Affected versions: Spring Web Services 5.0.0 through 5.0.1; 4.1.0 through 4.1.3; 4.0.0 through 4.0.18; 3.1.0 through 3.1.8.	2026-06-11	3.7	CVE-2026-41000
TwilN--gatus	A vulnerability was determined in TwilN gatus 5.36.0. Impacted is the function setSessionCookie of the file security/oidc.go of the component OIDC Session Cookie Handler. Executing a manipulation can lead to sensitive cookie without secure attribute. The attack can be launched remotely. This attack is characterized by high complexity. The exploitability is considered difficult. The reported GitHub issue was closed with the label "not planned".	2026-06-11	3.7	CVE-2026-11956
yoanbernabeu--grepai	A vulnerability was determined in yoanbernabeu grepai up to 0.35.0. The affected element is the function PostgresStore.LookupByContentHash of the file indexer/chunker.go of the component Postgres Embedding Cache. Executing a manipulation of the argument content_hash can lead to use of weak hash. The attack needs to be launched locally. The attack requires a high level of complexity. The exploitability is described as difficult. The exploit has been publicly disclosed and may be utilized. The pull request to fix this issue awaits acceptance.	2026-06-08	2.5	CVE-2026-11481
Black Lantern Security--BBOT	The docker_pull module uses the realm parameter from a Docker registry's WWW-Authenticate response header as the authentication endpoint without validation. An attacker in a man-in-the-middle position between bbot and a Docker registry could modify this header to redirect the authentication request to an arbitrary endpoint, potentially leaking authentication tokens.	2026-06-17	3.1	CVE-2026-12566
Black Lantern Security--BBOT	The github_workflows module constructs local directory paths from user-controlled repository names without validating for symlinks. A local attacker sharing the scan directory can plant a symlink at the predictable	2026-06-17	2.2	CVE-2026-12567

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	output path, causing workflow data to be written to an attacker-chosen location.			
Browerbase--Browserbase	A security flaw has been discovered in Browserbase up to 20260526. This impacts an unknown function of the component Autobrowse Trace Artifact Handler. The manipulation results in incorrect default permissions. The attack requires a local approach. The exploit has been released to the public and may be used for attacks. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	3.3	CVE-2026-12823
Capgo--Capgo	Capgo before 12.128.2 contains an authentication logic flaw: a user with permission to manage team or organization security settings can enable mandatory two-factor authentication for all team members without first enabling 2FA on their own account. The application fails to verify the initiator's 2FA status before allowing the policy change, resulting in inconsistent security enforcement, potential administrative misuse, and lockout risk for team members.	2026-06-20	3.8	CVE-2026-56212
Capgo--Capgo	Capgo before 12.128.2 uses ILIKE pattern matching instead of exact matching for app_id lookup in the preview subdomain resolver, allowing underscore characters in app_id to act as SQL wildcards. Attackers can create apps with app_ids differing by one character at underscore positions to cause unintended pattern matches, breaking preview functionality for legitimate apps or causing app-id confusion.	2026-06-20	3.1	CVE-2026-56325
Capgo--Capgo	Capgo before 12.128.2 contains an open redirect vulnerability in stripe_portal and stripe_checkout endpoints that accept unvalidated callbackUrl, successUrl, and cancelUrl parameters. Authenticated attackers can craft malicious billing URLs to redirect users to attacker-controlled domains for phishing and credential harvesting.	2026-06-20	3.5	CVE-2026-56330
Dell--PowerFlex	Dell PowerFlex Manager, version(s) [Versions], contain(s) an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with adjacent network access could potentially exploit this vulnerability, leading to information disclosure.	2026-06-17	3.5	CVE-2026-35068
GNU--Savane	GNU Savannah Administration Savane through 3.17 uses untrusted data as part of authorization.	2026-06-20	3.7	CVE-2026-56355
HCL Software--iControl	HCL iControl was affected by Inadequate Session Timeout vulnerability. The vulnerability involves a security risk where a web application fails to automatically terminate user sessions after a period of inactivity	2026-06-17	3.1	CVE-2025-62340
ImageMagick--ImageMagick	ImageMagick before 7.1.2-15 and 6.9.x before 6.9.13-40 contains an integer overflow in the PSB (PSD v2) RLE decoding path (ReadPSDChannelRLE in coders/psd.c) that causes a heap out-of-bounds read on 32-bit builds. Processing a crafted PSB file can lead to information disclosure or a crash.	2026-06-21	3.7	CVE-2026-56367
ImageMagick--ImageMagick	ImageMagick before 7.1.2-15 (and 6.x before 6.9.13-40) contains a heap out-of-bounds read in the PCD coder's DecodeImage loop. A crafted PCD file can trigger a one-byte heap out-of-bounds read during image decoding, resulting in denial of service and potential disclosure of an adjacent heap byte.	2026-06-21	3.7	CVE-2026-56378

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Intelbras--iNVU 7016 FT	A flaw has been found in Intelbras iNVU 7016 FT 3.004.00IB000.0.T Build 2025-09-26. This impacts an unknown function of the file /RPC2_Loadfile/syslog/ of the component Web Interface. Executing a manipulation can lead to path traversal. The attack can be launched remotely. The exploit has been published and may be used. It is recommended to upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.	2026-06-15	2.7	CVE-2026-12211
Intelliants--Subrion CMS	A vulnerability has been found in Intelliants Subrion CMS up to 4.0.3. Affected by this issue is some unknown functionality of the component Blocks Endpoint. Such manipulation of the argument CSS class name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-15	2.4	CVE-2026-12202
NI--grpc-device	There is an incorrect conversion between numeric types vulnerability in NI grpc-device due to missing range checks in CodeGen. This may silently discard high bits if a size value exceeded the target type's range. This affects NI grpc-device 2.17.0 and prior versions.	2026-06-19	3.7	CVE-2026-9143
OliveTin--OliveTin	OliveTin gives access to predefined shell commands from a web interface. In versions 3000.0.0 and prior, The ValidateArgumentType RPC endpoint in service/internal/api/api.go does not perform any authentication or authorization checks. Unlike all other data-returning API endpoints, it does not call auth.UserFromApiCall or checkDashboardAccess. When AuthRequireGuestsToLogin is enabled (the security-conscious configuration), this endpoint remains accessible to unauthenticated users and can be used as an oracle to enumerate valid action binding IDs and their argument configurations. This issue has been fixed in version 3000.13.0.	2026-06-15	3.7	CVE-2026-48709
Oracle Corporation--Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: VMSVGA device). The supported version that is affected is 7.2.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	2026-06-16	3.2	CVE-2026-46815
Oracle Corporation--Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: VMSVGA device). The supported version that is affected is 7.2.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	2026-06-16	3.2	CVE-2026-46816

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). The supported version that is affected is 7.2.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	2026-06-16	3.2	CVE-2026-46874
Oracle Corporation-- Oracle VM VirtualBox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: VMSVGA device). The supported version that is affected is 7.2.8. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 3.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).	2026-06-16	3.2	CVE-2026-46977
pgadmin.org-- pgAdmin 4	HTML injection in pgAdmin 4's cloud deployment module. The verify_credentials, deploy, regions, and update-server endpoints under /rds/, /azure/, /google/, and the top-level /cloud/ blueprint propagated AWS / Azure / Google SDK exception text - and the related file-resolution and database-commit exception text - into the JSON response body (the info and errmsg fields) without HTML-encoding. The Cloud Wizard frontend rendered these strings through html-react-parser, so an attacker-influenced exception message embedded structural HTML directly into the wizard's DOM. The reported entry point is /rds/verify_credentials/. An authenticated pgAdmin user submits a crafted access_key whose value contains an <iframe/src=...> payload; AWS STS rejects the credential with an IncompleteSignature exception whose text quotes the access_key verbatim; the pgAdmin backend forwards that text into the JSON info field; the Cloud Wizard's FormFooterMessage parses it as HTML. The browser fetches the iframe's src from an attacker-controlled host, and JavaScript executing inside the cross-origin iframe writes to parent.location, redirecting the victim's pgAdmin tab. Because the injection renders inside pgAdmin's own interface, X-Frame-Options and Content-Security-Policy frame-ancestors do not mitigate it. Baseline impact is self-targeted (the same user who supplied the payload sees the injection); escalation against other authenticated users requires an additional cross-site request-forgery primitive capable of submitting the malformed credential request with a valid X-pgA-CSRFToken in the victim's browser context. The same unsanitised-error-into-JSON pattern was present across multiple sibling endpoints - Azure's check_cluster_name_availability, every Google endpoint that surfaces SDK errors (verification_ack, projects, regions, instance_types, database_versions, the verify_credentials path-resolution branches), the central /deploy endpoint that bubbles str(e) from deploy_on_rds / deploy_on_azure / deploy_on_google, and update_cloud_server which surfaces the str(e) from a failing db.session.commit - all of which are now covered. Fix HTML-escapes every external/SDK exception string at the endpoint sink via a new shared	2026-06-18	3.5	CVE-2026-12047

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	sanitize_external_text helper (HTML escape with control-character strip), promoted out of the pycopg3 driver into web/pgadmin/utis/text_sanitize.py. The Cloud Wizard frontend additionally renders its FormFooterMessage in plain-text mode for backend-derived strings, so the value is never parsed as HTML even if a future sink forgets the escape. This issue affects pgAdmin 4: from 6.6 before 9.16.			
pointedilana--php-weasyprint	PhpWeasyPrint is a PHP library allowing PDF generation from a URL or an HTML page. Prior to version 2.6.0, `AbstractGenerator::\$temporaryFiles` is a public array, and `removeTemporaryFiles()` - invoked from `__destruct()` and from a registered shutdown function - calls `unlink()` on every entry without verifying that the path is contained within the temporary folder. Any code holding a reference to a generator instance can push an arbitrary path into the array and have it deleted on script shutdown. This mirrors the KnPLabs/snappy issue GHSA-87qc-37cw-84h4. PhpWeasyPrint version 2.6.0 contains a patch for the issue.	2026-06-19	3	CVE-2026-49358
Radware--Cyber Controller	A security vulnerability has been detected in Radware Cyber Controller up to 10.11.0. This affects an unknown part of the component HTML Report Generation. The manipulation leads to HTML injection. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-06-21	3.5	CVE-2026-12812
Snes9X team--Snes9X	snes9x 1.63 allows an out-of-bounds write and denial of service via a crafted .ups file.	2026-06-17	2.9	CVE-2026-39199
SteeltoeOSS--Steeltoe.Configuration.Encryption	Steeltoe is an open source project that provides a collection of libraries that helps users build cloud-native applications. In Steeltoe.Configuration.Encryption 4.0.0 through 4.1.0, configuring `encrypt:rsa:algorithm=OAEP` does not enable OAEP encryption. Due to an incorrect BouncyCastle transformation string, the `OAEP` setting selects PKCS#1 v1.5, which is the same algorithm as the `DEFAULT` setting. Steeltoe.Configuration.Encryption version 4.2.0 patches the issue.	2026-06-17	1.9	CVE-2026-50268
stiofansisland--UsersWP Front-end login form, User Registration, User Profile & Members Directory plugin for WP	The UsersWP - Front-end login form, User Registration, User Profile & Members Directory plugin for WP plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.2.63 via the 'user_id' parameter due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with editor-level access and above, to reset and permanently delete the avatar or banner image of any arbitrary user, including administrators, by clearing their avatar_thumb or banner_thumb metadata in the uwp_usermeta table.	2026-06-18	2.7	CVE-2026-12102
undici--undici	Impact: When undici parses a Set-Cookie header, it accepts any SameSite attribute value that contains Strict, Lax, or None as a substring, rather than the case-insensitive exact match specified by RFC 6265. Non-spec values are silently mapped to one of the three standard tokens. For example, SameSite=NoneOfYourBusiness is parsed as None (the most permissive setting), and SameSite=StrictLax is parsed as Lax (a downgrade from Strict). Affected applications are those that consume Set-Cookie headers from server responses (for example via undici's fetch or proxy code paths) and then forward or rely on the parsed sameSite attribute. A malicious or non-	2026-06-17	3.7	CVE-2026-11525

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	compliant server can coerce the consumer's view of a cookie's SameSite policy to a weaker value, silently degrading the SameSite enforcement the cookie is supposed to provide. This was introduced in undici 5.15.0 when the cookies feature was added. Patches: Upgrade to undici v6.26.0, v7.28.0 or v8.5.0. Workarounds: After parsing a Set-Cookie header, validate that the resulting sameSite attribute is one of 'Strict', 'Lax', or 'None' (exact, case-insensitive) before forwarding or relying on it.			
undici--undici	Impact: Undici's HTTP/1.1 client is vulnerable to response queue poisoning on reused keep-alive sockets. An attacker-controlled upstream server can inject an unsolicited HTTP/1.1 response onto an idle socket after a request completes. When the client dispatches the next request on that socket, it associates the injected response with the new request, causing responses to be delivered to the wrong requests. This requires an attacker-controlled or compromised upstream HTTP/1.1 server and keep-alive connection reuse. Patches: Upgrade to undici v6.26.0, v7.28.0 or v8.5.0. Workarounds: Disable keep-alive connection reuse by setting keepAliveTimeout: 0 on the Client or Pool.	2026-06-17	3.7	CVE-2026-6733
zephyrproject--zephyr	In Zephyr's IPv4 IGMP implementation, igmp_send() in subsys/net/ip/igmp.c read the network interface back out of the packet via net_pkt_iface(pkt) after the packet had been handed to net_send_data(). On the successful-send path the packet's last reference may already have been released by the L2 driver or by the network stack's TX handling (synchronously in the default NET_TC_TX_COUNT=0 immediate-transmit configuration), returning the net_pkt slab block to its free list. The subsequent net_pkt_iface(pkt) dereferences the freed packet, a use-after-free read; with CONFIG_NET_STATISTICS_PER_INTERFACE the resulting dangling interface pointer is further dereferenced for a statistics-counter write. The IGMP send path is reachable without authentication from inbound IPv4 IGMP membership queries addressed to 224.0.0.1 (net_ipv4_igmp_input - send_igmp_report/send_igmp_v3_report - igmp_send), as well as from local multicast join/leave/rejoin operations. Realistic impact is undefined behavior and potential denial of service (sporadic crash or stats corruption); a controllable write requires the asynchronous TX path plus a concurrent slab reuse. The flaw was introduced with IGMPv2 support and affects releases from v2.6.0 through v4.4.0. The fix caches the interface pointer before sending. Note the analogous IPv6 MLD path (mld_send in subsys/net/ip/ipv6_mld.c) retains the same unfixed pattern.	2026-06-16	3.7	CVE-2026-10636
7-Zip--7-Zip	7-Zip for Windows through 26.02 fails to preserve the Mark-of-the-Web when extracting a crafted RAR5 archive, because its guard that suppresses an archive-supplied Zone.Identifier stream matches the exact name 'Zone.Identifier' while a RAR5 STM record named ':Zone.Identifier:\$DATA' is not matched and NTFS canonicalizes it to the same stream, overwriting the propagated Internet-zone marker with ZoneId=0. A second STM record named '::\$DATA' overwrites the extracted file's default data stream, letting an attacker defeat SmartScreen/MotW warnings and spoof file content.	2026-06-28	3.3	CVE-2026-58052
78--xiaozihi-esp32	A weakness has been identified in 78 xiaozihi-esp32 up to 2.2.6. Affected by this issue is the function ParseMessage of the file main/mcp_server.cc of the component MCP Response Handler. This manipulation causes improper synchronization. Remote exploitation of the attack is possible. The attack's complexity is rated as high. The exploitation is known to be	2026-06-28	3.1	CVE-2026-13489

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	difficult. The exploit has been made available to the public and could be used for attacks. The pull request to fix this issue awaits acceptance.			
78--xiaozi-esp32	A vulnerability was detected in 78 xiaozi-esp32 up to 2.2.6. This vulnerability affects the function Application::GetInstance of the file main/protocols/mqtt_protocol.cc of the component MQTT Goodbye Handler. Performing a manipulation of the argument session_id results in denial of service. The attack is possible to be carried out remotely. The complexity of an attack is rather high. It is stated that the exploitability is difficult. The exploit is now public and may be used. The patch is named e182471f8c5a22434346bd98da34d3b66c8c8b3e. It is recommended to apply a patch to fix this issue.	2026-06-28	3.7	CVE-2026-13491
AIDC-AI--ComfyUI-Copilot	A flaw has been found in AIDC-AI ComfyUI-Copilot up to 2.0.28. This issue affects some unknown processing of the file backend/controller/conversation_api.py of the component Workflow Checkpoint Restore Handler. Executing a manipulation can lead to improper control of resource identifiers. The attack may be performed from remote. A high complexity level is associated with this attack. The exploitability is assessed as difficult. The exploit has been published and may be used. The pull request to fix this issue awaits acceptance.	2026-06-28	3.1	CVE-2026-13493
arc53--DocsGPT	A flaw has been found in arc53 DocsGPT up to 0.18.0. The affected element is the function encrypt_credentials of the file application/security/encryption.py of the component Credential Storage. This manipulation causes insufficient verification of data authenticity. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is described as difficult. The exploit has been published and may be used. The pull request to fix this issue awaits acceptance.	2026-06-28	3.1	CVE-2026-13483
babel--babel	Babel is a compiler for writing next generation JavaScript. Prior to 8.0.0-rc.6 and 7.29.6, @babel/core affected by an arbitrary file read via a sourceMappingURL comment. Using @babel/core to compile maliciously crafted code can allow an attacker to read any source map from the system that is running Babel, if the attacker controls the input source code, can read the output source code, and knows the path of the source map file that they want to read. This vulnerability is fixed in 8.0.0-rc.6 and 7.29.6.	2026-06-22	3.2	CVE-2026-49356
bitwarden--server	Bitwarden Server before 2026.5.0 contains a JSON injection vulnerability in IntegrationTemplateProcessor.ReplaceTokens(), which substitutes user-controlled values into event-integration templates without JSON encoding. When an organization has configured an event integration whose template references a user-controlled token (such as #ActingUserName# or #UserName#, populated from a member's display name), an authenticated member can set their display name to JSON metacharacters and inject arbitrary key-value pairs into the rendered payloads delivered to webhook, SIEM, Slack, Teams, or Datadog endpoints, making injected fields indistinguishable from legitimate template output.	2026-06-25	3.5	CVE-2026-57522
Cacti--cacti	Cacti is an open source performance and fault management framework. In versions 1.2.30 and below, the locale-dependent decimal formatting in rrdtool_function_update() can corrupt RRDtool metric values. The rrdtool_function_update() function checks metric values with is_numeric()	2026-06-24	2.9	CVE-2026-39894

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and concatenates them into the RRDtool update command via PHP string interpolation. PHP's string cast of floats is locale-sensitive: if LC_NUMERIC uses comma as decimal separator (e.g., de_DE), a value of 1.5 becomes "1,5". RRDtool expects . as decimal separator, causing metric data to shift into wrong columns or be silently dropped. No setlocale() reset is present in the update path. This causes a data integrity issue, but is not remotely exploitable; it requires server locale misconfiguration. The issue has been fixed in version 1.2.31.			
Chess--Play and Learn App	A weakness has been identified in Chess Play and Learn App up to 4.9.42 on Android. This issue affects some unknown processing of the file AndroidManifest.xml of the component com.chess. This manipulation causes exposure of backup file to an unauthorized control sphere. It is feasible to perform the attack on the physical device. The exploit has been made available to the public and could be used for attacks. Upgrading the affected component is advised. The vendor was informed early about this issue. They confirmed the existence and that they will address it. Furthermore, they explain that their bug bounty "explicitly excludes physical-access attacks". However, they appreciate the quality of the report and aim at making a goodwill payment to the researcher.	2026-06-28	2.4	CVE-2026-13514
code-projects--Project Management System	A vulnerability has been found in code-projects Project Management System 1.0. This vulnerability affects unknown code of the file /mail.php of the component Mail Compose Page. Such manipulation leads to cross site scripting. The attack may be performed from remote. The exploit has been disclosed to the public and may be used.	2026-06-28	3.5	CVE-2026-13504
earendil-works--pi	Pi is a minimal terminal coding harness. From 0.74.0 until 0.78.1, Pi HTML exports render session Markdown into a static HTML file. It did not consistently reject unsafe Markdown link and image URL schemes. In versions with scheme filtering, C0 control characters in the URL scheme could bypass the check because browsers normalize those characters before navigation. This vulnerability is fixed in 0.78.1.	2026-06-23	2.5	CVE-2026-54326
earendil-works--pi	Pi is a minimal terminal coding harness. From 0.74.0 until 0.78.1, Pi stored API keys and OAuth credentials in auth.json. A race condition in the file write path could briefly create or rewrite this file with permissions derived from the process umask before tightening the file to owner-only permissions. This vulnerability is fixed in 0.78.1.	2026-06-23	2.2	CVE-2026-54327
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 17.9 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1 that under certain conditions could have allowed an authenticated user with custom role permissions to view, create, or delete protected environment configurations despite CI/CD visibility being disabled for the project.	2026-06-25	3.8	CVE-2026-0934
GitLab--GitLab	GitLab has remediated an issue in GitLab EE affecting all versions from 18.6 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1 that under certain conditions could have allowed an authenticated user with limited permissions to access project information due to insufficient authorization checks.	2026-06-25	3.1	CVE-2026-3176
glpi-project--glpi	A security vulnerability has been detected in glpi-project glpi 11.0.5/11.0.6/11.0.7. This affects the function Document::canViewFile of the file front/document.send.php of the component Document Handler. Such manipulation of the argument docid leads to authorization bypass.	2026-06-28	3.7	CVE-2026-13490

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The attack can be executed remotely. This attack is characterized by high complexity. It is indicated that the exploitability is difficult. The vendor was contacted early about this disclosure.			
GNU--GNU SASL	GNU SASL before 2.2.4 lacks sanitization of a short challenge in _gsasl_ntlm_client_step in the NTLM client, which could result in memory disclosure via a crafted server.	2026-06-23	3.7	CVE-2026-56968
GnuPG--GnuPG	CMS (Cryptographic Message Syntax) parsing in gpgsm in GnuPG through 2.5.20 mishandles the CMS format for AES-GCM because aes-ICVlen is supposed to be 12 bytes but 4 bytes is accepted. NOTE: this is related to CVE-2026-34182.	2026-06-23	2.9	CVE-2026-57062
gogs--gogs	Gogs is an open source self-hosted Git service. Prior to 0.14.3, specially crafted issue index pattern can cause a panic when rendering, resulting in denial of service. In internal/markup/markup.go, RenderIssueIndexPathPattern renders the issue index pattern to a link using com.Expand, which is not safe: when the configured pattern contains an opening brace { but no closing brace }, strings.Index(template, "{") returns -1 and the subsequent slice template[: -1] triggers a panic. Once such a pattern is set, any page in the affected repository that contains an issue index reference such as #1 becomes unavailable. This vulnerability is fixed in 0.14.3.	2026-06-24	3.5	CVE-2026-52796
HCLSoftware--Connections	HCL Connections contains a broken access control vulnerability that may allow an unauthorized user to view data in a single specific scenario.	2026-06-23	3.5	CVE-2025-15619
IBM--Datacap	IBM Datacap 9.1.7, 9.1.8, and 9.1.9 and IBM Datacap Navigator 9.1.7, 9.1.8, and 9.1.9 exposes resources or functionality that isn't linked in the UI but is accessible by directly requesting the URL, bypassing intended access controls.	2026-06-22	2.3	CVE-2026-9610
ImageMagick--ImageMagick	ImageMagick before 7.1.2-15 contains a memory leak vulnerability in multiple coders that write raw pixel data where allocated objects are not properly freed. Attackers can trigger this leak by processing specially crafted images, causing memory exhaustion and denial of service.	2026-06-24	3.7	CVE-2026-56368
ImageMagick--ImageMagick	ImageMagick before 7.1.2-19 contains an out-of-bounds access vulnerability in ConnectedComponentsImage() when processing connected-components artifacts with invalid indices. Attackers can trigger access violations by specifying malformed connected-components definitions via CLI, causing denial of service or potential code execution.	2026-06-24	3.3	CVE-2026-56370
ImageMagick--ImageMagick	ImageMagick before 7.1.2-15 and 6.9.13-40 contains a heap use-after-free in the meta coder: when memory allocation fails, a single byte is written to a stale pointer. Remote attackers can trigger it by processing specially crafted image files, causing a denial of service.	2026-06-23	3.7	CVE-2026-56376
JetBrains--YouTrack	In JetBrains YouTrack before 2026.2.16593 project settings disclosure via the MCP was possible	2026-06-26	3.1	CVE-2026-57922
JetBrains--YouTrack	In JetBrains YouTrack before 2026.2.16593 the websandbox bridge was vulnerable to a prototype pollution attack	2026-06-26	2.6	CVE-2026-57926
Kludex--python-multipart	Python-Multipart is a streaming multipart parser for Python. Prior to 0.0.30, parse_options_header parsed Content-Disposition (and Content-Type) headers with email.message.Message, which transparently applies RFC 2231/5987 decoding. The extended parameter syntax	2026-06-22	3.7	CVE-2026-53537

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	(filename*=charset'lang'value, name*=..., and the filename*0/filename*1 continuation form) is decoded and surfaced under the bare filename/name key, and overrides the plain parameter when both are present. RFC 7578 §4.2 explicitly forbids the filename* form in multipart/form-data. Components that follow RFC 7578, or that do not implement RFC 2231/5987 decoding for multipart/form-data (WAFs, proxies, gateways), may interpret such a header differently. An attacker can exploit that difference to smuggle a different field name or filename past an upstream inspector to the backend. This vulnerability is fixed in 0.0.30.			
Kludex--python-multipart	Python-Multipart is a streaming multipart parser for Python. Prior to 0.0.30, QuerystringParser treated ; as a field separator in application/x-www-form-urlencoded bodies, in addition to &. The WHATWG URL standard, modern browsers, and Python's urllib.parse (since the CVE-2021-23336 fix) treat only & as a separator. This creates a parser differential: the same bytes are tokenized into different fields than a WHATWG compliant intermediary would produce, allowing an attacker to smuggle extra form fields past an upstream body inspecting component. This vulnerability is fixed in 0.0.30.	2026-06-22	3.7	CVE-2026-53538
Kludex--python-multipart	Python-Multipart is a streaming multipart parser for Python. Prior to 0.0.31, parse_form() did not validate the Content-Length header before using it to bound its chunked read of the request body. A negative Content-Length turned the bounded read into a read-until-EOF, so the entire body was loaded into memory in a single read instead of in fixed-size chunks. This vulnerability is fixed in 0.0.31.	2026-06-22	3.7	CVE-2026-53540
Kludex--starlette	Starlette is a lightweight ASGI framework/toolkit. Prior to 1.3.0, the HTTP request path is not validated before being used to reconstruct request.url. Because request.url is rebuilt by concatenating {scheme}://{host}{path} and re-parsing the result, a path that does not begin with / (for example @google.com) moves the authority boundary during re-parsing, so request.url.hostname and request.url.netloc become attacker-controlled. Code that reads request.url.hostname (rather than the Host header or scope) can therefore be misled into trusting an attacker-supplied host. This vulnerability is fixed in 1.3.0.	2026-06-22	3.7	CVE-2026-54282
Mattermost--Mattermost	Mattermost versions 10.11.x <= 10.11.18, 11.6.x <= 11.6.3, 11.5.x <= 11.5.6 fail to properly apply markdown image rendering restrictions to AI bot tool result posts, which allows an authenticated attacker to exfiltrate data to an attacker-controlled server via injecting markdown image syntax into tool result content rendered by a victim's client.. Mattermost Advisory ID: MMSA-2026-00619	2026-06-26	3.5	CVE-2026-3472
Mattermost--Mattermost	Mattermost versions 11.7.x <= 11.7.0, 10.11.x <= 10.11.17 fail to enforce bot-specific permission checks on the user active status endpoint, which allows a User Manager with user management write access but no Integrations access to deactivate bot accounts via the PUT /api/v4/users/{id}/active API endpoint.. Mattermost Advisory ID: MMSA-2026-00667	2026-06-22	3.8	CVE-2026-8074
Mattermost--Mattermost	Mattermost versions 11.7.x <= 11.7.0, 10.11.x <= 10.11.17 fail to validate bot targets when demoting users to guests which allows a lower-privileged	2026-06-22	3.8	CVE-2026-8823

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	administrator to degrade arbitrary bot accounts via the standard demote-user API.. Mattermost Advisory ID: MMSA-2026-00669			
nocodb--nocodb	NocoDB is software for building databases as spreadsheets. Prior to 2026.04.1, the OAuth token strategy attached oauth_scope and oauth_granted_resources to the request user, but the ACL middleware never consulted either. An OAuth token issued with a restricted scope (e.g. MCP-only) therefore inherited the full permissions of the underlying user across all routes; the granted_resources.base_id restriction was bypassed on org-level endpoints that don't populate req.context.base_id. This vulnerability is fixed in 2026.04.1.	2026-06-23	2	CVE-2026-46549
PowerDNS--DNSdist	An attacker sending a large number of crafted DNS queries might be able to trigger a dynamic block being inserted with a value causing invalid output to be produced in the prometheus endpoint. The prometheus endpoint will then be rejected by the scraper until the dynamic block expires.	2026-06-25	3.7	CVE-2026-40011
PowerDNS--DNSdist	An attacker might be able to delay the processing of DoH3 queries by sending DoH3 GET queries with an invalid DATA frame.	2026-06-25	3.7	CVE-2026-40208
PowerDNS--DNSdist	An attacker can send a crafted EDNS OPT record that will be ignored by DNSdist's filtering rules, but will be rewritten as a valid OPT record when EDNS Client Subnet is inserted, causing the backend to see the EDNS option(s) that DNSdist did not filter.	2026-06-25	3.7	CVE-2026-42004
Rapid7--InsightConnect Compression Plugin	Path Traversal vulnerability in the create_archive function of Rapid7 InsightConnect Compression Plugin on Linux allows authenticated attackers to write to unintended file paths via crafted filename input. The impact is limited to file corruption as content cannot be controlled by the attacker.	2026-06-25	3.3	CVE-2026-8662
Red Hat--Red Hat Enterprise Linux 10	A flaw was found in OpenSSH. This vulnerability, a heap out-of-bounds read, occurs during the cleanup of GSSAPI (Generic Security Service Application Programming Interface) indicators when a trailing NULL termination is missing in the auth-indicators array. A remote attacker, under specific configurations involving GSSAPI authentication and a Kerberos environment, could exploit this to cause the SSH authentication path to crash or abort. This leads to a denial of service (DoS), impacting the availability of the SSH service.	2026-06-23	3.7	CVE-2026-55654
Red Hat--Red Hat OpenShift Virtualization 4	A flaw was found in KubeVirt's downward metrics virtio-serial server. The server reads guest requests using textproto.Reader.ReadLine(), which buffers input indefinitely until a newline character is received, with no length limit or read deadline. A user with access to a VM guest that has the downward metrics virtio-serial device configured can write a continuous byte stream to the device, causing unbounded memory allocation in the virt-handler process until it is OOM-killed.	2026-06-26	3.8	CVE-2026-13322
remix-run--react-router	React Router is a router for React. From 7.12.0 until 7.15.1, certain CSRF checks in React Router v7 Framework Mode were insufficient and run on POST requests, but were bypassed on PUT/PATCH/DELETE requests. This is a low severity vulnerability because modern browser protections (CORS preflight, SameSite cookies) already block the cross-origin attack vectors	2026-06-22	3.1	CVE-2026-53663

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	that this missing CSRF check would otherwise gate. This vulnerability is fixed in 7.15.1.			
SimStudioAI--sim	A vulnerability was found in SimStudioAI sim up to 0.6.92. Affected by this vulnerability is an unknown functionality in the library apps/sim/lib/core/security/deployment.ts of the component Password Protection Handler. Performing a manipulation results in use of weak hash. The attack is possible to be carried out remotely. The attack's complexity is rated as high. The exploitation appears to be difficult. The exploit has been made public and could be used. The pull request to fix this issue awaits acceptance.	2026-06-28	3.7	CVE-2026-13510
skypilot-org--skypilot	A vulnerability was detected in skypilot-org skypilot up to 0.12.0. Impacted is the function username.encode of the file sky/users/server.py of the component User ID Handler. The manipulation results in use of weak hash. The attack may be performed from remote. This attack is characterized by high complexity. The exploitability is considered difficult. The exploit is now public and may be used. The vendor was contacted early about this disclosure.	2026-06-28	3.7	CVE-2026-13482
sparklemotion--nokogiri	Nokogiri is an open source XML and HTML library for the Ruby programming language. Prior to 1.19.4, the NONET parse option, which Nokogiri turns on by default for Nokogiri::XML::Schema (see CVE-2020-26247), was not correctly enforced on the JRuby implementation. As a result, a schema parsed with default options could still cause external resources to be fetched over the network, potentially enabling SSRF or XXE attacks. This vulnerability is fixed in 1.19.4.	2026-06-25	2.6	CVE-2026-57234
tenable--Nessus	A SQL injection vulnerability in Nessus allows an attacker to craft a malicious scan result file that, when imported by a privileged user, injects malicious SQL into the scan results database, potentially enabling exfiltration of scan-result data.	2026-06-25	3.3	CVE-2026-57588
VoltAgent--VoltAgent	A vulnerability was determined in VoltAgent up to 2.1.17. Affected by this issue is the function handleGetMemoryConversation of the file packages/server-core/src/handlers/memory.handlers.ts of the component Memory REST API. Executing a manipulation of the argument conversationId can lead to improper authorization. The attack may be performed from remote. This attack is characterized by high complexity. The exploitation is known to be difficult. The exploit has been publicly disclosed and may be utilized. The pull request to fix this issue awaits acceptance.	2026-06-28	3.1	CVE-2026-13511
code-projects--Assessment Management	A weakness has been identified in code-projects Assessment Management 1.0. Affected by this issue is some unknown functionality of the file admin/view-users.php. Executing a manipulation of the argument User can lead to cross site scripting. The attack may be performed from remote. The exploit has been made available to the public and could be used for attacks.	2026-07-04	2.4	CVE-2026-14655
CodeAstro--Complaint Management System	A security flaw has been discovered in CodeAstro Complaint Management System 1.0. This issue affects some unknown processing of the file /report/addreport of the component Report Handler. Performing a manipulation of the argument Report Title results in cross site scripting.	2026-06-29	3.5	CVE-2026-13558

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Remote exploitation of the attack is possible. The exploit has been released to the public and may be used for attacks.			
connorskees--grass	A flaw has been found in connorskees grass up to 0.13.4. The affected element is the function grass_compiler::raw_to_parse_error of the component UTF-8 Character Handler. Executing a manipulation can lead to denial of service. The attack is restricted to local execution. The exploit has been published and may be used. In Issue #117 with similar structure the project maintainer explains: "DoS vulnerabilities are generally fine in Sass compilers -- they are trivially possible with recursive functions, infinite loops, nested mixins, etc. The description here is wrong. Compile time is not expected to be linear relative to the input, and the @extend algorithm is definitionally exponential."	2026-07-04	3.3	CVE-2026-14650
connorskees--grass	A vulnerability has been found in connorskees grass up to 0.13.4. The impacted element is the function grass_compiler::selector::extend/grass_compiler::evaluate::visitor. The manipulation leads to denial of service. The attack must be carried out locally. The exploit has been disclosed to the public and may be used. The project maintainer explains: "DoS vulnerabilities are generally fine in Sass compilers -- they are trivially possible with recursive functions, infinite loops, nested mixins, etc. The description here is wrong. Compile time is not expected to be linear relative to the input, and the @extend algorithm is definitionally exponential."	2026-07-04	3.3	CVE-2026-14651
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an use of uninitialized resource vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to information exposure.	2026-07-03	3.3	CVE-2026-56085
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.6, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an Improper limitation of a pathname to a restricted directory ('path traversal') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure.	2026-07-03	2.3	CVE-2026-41124
Dell--PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7, LTS2026 release version 8.6.1.0 through 8.6.1.10, LTS2025 release version 8.3.1.0 through 8.3.1.30, LTS2024 release versions 7.13.1.0 through 7.13.1.70 contain an use of less trusted source vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to information tampering.	2026-07-03	2.7	CVE-2026-46466
exo-explore--exo	A security flaw has been discovered in exo-explore exo up to 1.0.71. Affected is the function _image_cache_key of the file src/exo/worker/engines/mlx/vision.py of the component Vision Feature Cache. The manipulation results in use of weak hash. It is possible to launch the attack remotely. A high complexity level is associated with this attack. The exploitability is told to be difficult. The exploit has been released to the public and may be used for attacks. The pull request to fix this issue awaits acceptance.	2026-07-05	3.7	CVE-2026-14738

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
FederatedAI--FATE	A vulnerability has been found in FederatedAI FATE up to 2.2.0. This affects the function QueuePushReqStreamObserver.initEggroll of the file java/osx/osx-broker/src/main/java/org/fedai/osx/broker/grpc/QueuePushReqStreamObserver.java of the component OSX Broker. Such manipulation of the argument rollSiteSessionId/dstRole/dstPartyId leads to exposure of data element to wrong session. The attack can be executed remotely. A high complexity level is associated with this attack. It is indicated that the exploitability is difficult. The exploit has been disclosed to the public and may be used. The pull request to fix this issue awaits acceptance.	2026-07-04	3.1	CVE-2026-14621
ForceInjection--AI-fundermentals	A vulnerability has been found in ForceInjection AI-fundermentals 2.0/3.0. Affected by this vulnerability is the function get_conversation_history of the file 08_agentic_system/memory/langchain/code/smart_customer_service.py of the component Memory Recall Handler. The manipulation leads to use of weak hash. Remote exploitation of the attack is possible. A high degree of complexity is needed for the attack. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The identifier of the patch is f57277fdd9ba373ace72d83c272023ec67f720d6. It is suggested to install a patch to address this issue. The project confirms (translated from Chinese): "We now require session ownership verification in methods such as `username`, `sessionowner`, etc., and we've chat()changed the generation of `sessionowner` to include verified user identity and security context metadata."	2026-07-04	3.1	CVE-2026-14630
GPAC--GPAC	A weakness has been identified in GPAC up to 26.02.0. This affects an unknown part of the file src/utls/base_encoding.c of the component ISOBMFF Parser. Executing a manipulation can lead to highly compressed data. The attack needs to be launched locally. The exploit has been made available to the public and could be used for attacks. This patch is called 297f2d8d1f493d8b241330533cd47f7da758aeb3. A patch should be applied to remediate this issue. The vendor confirms: "We added a check on inflate output size, if it surpasses 32 times the input size we stop in error. This value could be adjusted later."	2026-06-29	3.3	CVE-2026-13523
HdrHistogram--HdrHistogram	A vulnerability was detected in HdrHistogram up to 2.2.2. Affected by this issue is the function org.HdrHistogram.AbstractHistogram.decodeFromCompressedByteBuffer of the file src/main/java/org/HdrHistogram/AbstractHistogram.java. The manipulation of the argument lengthOfCompressedContents results in uncontrolled memory allocation. The attack needs to be approached locally. The exploit is now public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-07-04	3.3	CVE-2026-14683
HdrHistogram--HdrHistogram	A flaw has been found in HdrHistogram up to 2.2.2. This affects the function org.HdrHistogram.AbstractHistogram.decodeFromByteBuffer of the file src/main/java/org/HdrHistogram/AbstractHistogram.java. This manipulation of the argument numberOfSignificantValueDigits causes uncontrolled memory allocation. The attack can only be executed locally. The exploit has been published and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-07-04	3.3	CVE-2026-14684

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
HdrHistogram-- HdrHistogram	A vulnerability has been found in HdrHistogram up to 2.2.2. This vulnerability affects the function recordValueWithCount of the file src/main/java/org/HdrHistogram/AbstractHistogram.java of the component AbstractHistogram. Such manipulation of the argument Count leads to state issue. The attack can only be performed from a local environment. The exploit has been disclosed to the public and may be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-07-04	3.3	CVE-2026-14685
HdrHistogram-- HdrHistogram	A vulnerability was found in HdrHistogram up to 2.2.2. This issue affects the function org.HdrHistogram.DoubleHistogram.recordValue of the file src/main/java/org/HdrHistogram/DoubleHistogram.java of the component Range Check. Performing a manipulation results in incorrect comparison. The attack is only possible with local access. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-07-05	3.3	CVE-2026-14686
Hitachi--Hitachi Virtual Storage Platform One Block 23, 24, 26, 28	Lack of validation for firmware update in Hitachi Hitachi Virtual Storage Platform One Block 23, 24, 26, 28. This issue affects Hitachi Virtual Storage Platform One Block 23, 24, 26, 28: before DKCMAIN A3-04-21-40/00, ESM A3-04-21/00.	2026-06-29	3.7	CVE-2025-0824
IBM--InfoSphere Information Server	IBM InfoSphere Information Server 11.7.0.0 through 11.7.1.6 is affected by an information disclosure vulnerability.	2026-06-30	3.5	CVE-2026-9836
ImageMagick-- ImageMagick	ImageMagick before 7.1.2-19 contains an off-by-one error in morphology validation allowing out-of-bounds heap buffer reads. Attackers can trigger heap buffer overflow by providing incorrect morphology parameters causing single pixel memory access violations.	2026-06-30	3.3	CVE-2026-56361
ImageMagick-- ImageMagick	ImageMagick before 7.1.2-22 contains a division by zero vulnerability in binomial kernel processing that allows attackers to cause denial of service. An attacker can supply a large binomial kernel value causing integer overflow, resulting in division by zero and application crash.	2026-06-30	3.3	CVE-2026-56363
ImageMagick-- ImageMagick	ImageMagick before 7.1.2-19 contains a memory leak vulnerability in the PNG encoder when writing MNG images. Attackers can trigger the encoder failure condition to exhaust memory resources and cause denial of service.	2026-06-30	3.7	CVE-2026-56365
ImageMagick-- ImageMagick	ImageMagick before 7.1.2-22 contains an information disclosure vulnerability in the PasskeyEncipherImage method due to AES-CTR nonce reuse. Attackers can exploit nonce reuse in the cipher implementation to recover plaintext information from encrypted images.	2026-06-30	3.7	CVE-2026-56369
ImageMagick-- ImageMagick	ImageMagick before 7.1.2-24 contains an incorrect policy check that allows attackers to create or truncate files disallowed by security policies. Remote attackers can bypass path policy restrictions in sandboxed conversion services to write arbitrary files outside intended boundaries.	2026-06-30	3.3	CVE-2026-56377
ImageMagick-- ImageMagick	ImageMagick before 7.1.2-13 contains a memory leak vulnerability in LoadOpenCLDeviceBenchmark() function when parsing malformed OpenCL device profile XML files with unclosed device elements. Attackers with write access to the OpenCL cache directory can place malicious XML files to exhaust memory and cause denial of service.	2026-06-30	1.9	CVE-2026-56364

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
iv-org--Invidious	Invidious before version 2.20260626.0 contains a broken access control vulnerability that allows unauthenticated attackers to retrieve private playlist contents by accessing the RSS feed playlist endpoint without authentication. Attackers can supply a playlist ID to the feed endpoint to obtain the full playlist contents, owner email address, and associated video entries without any authentication.	2026-06-29	3.7	CVE-2026-57946
langchain-ai--langgraph	A vulnerability was determined in langchain-ai langgraph up to 1.2.4. The affected element is the function _freeze of the file libs/langgraph/langgraph/_internal/_cache.py of the component Task Result Cache. This manipulation of the argument default_cache_key causes use of weak hash. The attack is possible to be carried out remotely. The complexity of an attack is rather high. The exploitability is described as difficult. The exploit has been publicly disclosed and may be utilized. The pull request to fix this issue awaits acceptance.	2026-07-05	3.1	CVE-2026-14742
llvm--llvm-project	A vulnerability was found in llvm llvm-project up to 22.1.6. This affects the function llvm::StringMap::insert in the library /lib/IR/ValueSymbolTable.cpp of the component ValueSymbolTable Module. The manipulation results in stack-based buffer overflow. Attacking locally is a requirement. The exploit has been made public and could be used. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-29	3.3	CVE-2026-13573
llvm--llvm-project	A vulnerability was determined in llvm llvm-project up to 22.1.6. This impacts the function GCRelocateInst::getBasePtr in the library llvm/lib/IR/IntrinsicInst.cpp of the component Bitcode File Handler. This manipulation causes heap-based buffer overflow. It is possible to launch the attack on the local host. The exploit has been publicly disclosed and may be utilized. The project was informed of the problem early through an issue report but has not responded yet.	2026-06-29	3.3	CVE-2026-13574
mjperpinosa--stumasy	A security vulnerability has been detected in mjperpinosa stumasy up to 327d1b0f2915ba79d7ef8ebb74553e987609d9be. This affects the function add_definition of the file application/PHP/objects/notes/add_into_dictionary.php. Such manipulation of the argument reference leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed publicly and may be used. This product takes the approach of rolling releases to provide continuous delivery. Therefore, version details for affected and updated releases are not available. The project was informed of the problem early through an issue report but has not responded yet.	2026-07-05	3.5	CVE-2026-14752
NousResearch--hermes-agent	A security vulnerability has been detected in NousResearch hermes-agent up to 2026.4.30. Affected is the function GatewayStreamConsumer._filter_and_accumulate of the file gateway/stream_consumer.py of the component Streaming Reasoning Tag Filter. The manipulation leads to improper handling of case sensitivity. The attack may be initiated remotely. The attack's complexity is rated as high. The exploitability is told to be difficult. The exploit has been disclosed publicly and may be used. The project decided to not implement a dedicated fix: "[T]he analysis and the fix are both sound. It just lands below the bar for the maintenance cost of a duplicated scrub path."	2026-07-03	3.1	CVE-2026-14617

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
opencontainers--runc	runc is a CLI tool for spawning and running containers according to the OCI specification. In versions prior to 1.3.6, 1.4.0-rc.1, 1.4.0-rc.12, 1.5.0-rc.1, and 1.5.0-rc.1, when setting up the container rootfs, setupPtmx and setupDevSymlinks call os.Remove and os.Symlink with a filepath.Join string which allow an image with /dev as a symlink to trick runc into deleting files called ptmx on the host or creating a hardcoded set of symlinks with specific names and targets in an arbitrary pre-existing host directory. This issue is not exploitable under Docker, because Docker creates a top-level read-only layer that masks any malicious /dev symlink present in the container image - unlike some other Linux container tooling, whose higher-level runtimes built on runc remain exposed to exploitation via a malicious image. This issue has been fixed in versions 1.3.6, 1.4.3 and 1.5.0.	2026-07-01	3.3	CVE-2026-41579
radareorg--radare2	A vulnerability was identified in radareorg radare2 up to 6.1.6. This vulnerability affects the function cmd_anal_opcode of the file libr/core/cmd_anal.inc.c of the component hexpairs Parser. Such manipulation leads to integer overflow. The attack needs to be performed locally. The exploit is publicly available and might be used. The name of the patch is 84e773986e7e5bb30453a9384f498ec0ccc9d0a9. A patch should be applied to remediate this issue.	2026-07-05	3.3	CVE-2026-14758
radareorg--radare2	A security flaw has been discovered in radareorg radare2 up to 6.1.6. This issue affects the function r_bin_java_inner_classes_attr_calc_size of the file shlr/java/class.c of the component RBinJava Line Number Table Parser. Performing a manipulation results in heap-based buffer overflow. The attack requires a local approach. The exploit has been released to the public and may be used for attacks. The patch is named cd62d15a6cbecdc67fd03f3ebdbbbbeb741d18f87. To fix this issue, it is recommended to deploy a patch.	2026-07-05	3.3	CVE-2026-14759
radareorg--radare2	A weakness has been identified in radareorg radare2 up to 6.1.6. Impacted is the function r_core_seek_arch_bits of the file libr/core/disasm.c of the component regprofile Handler. Executing a manipulation can lead to use after free. The attack requires local access. The exploit has been made available to the public and could be used for attacks. This patch is called 8b25c773785d85cb0103410a0905089d286921c2. It is advisable to implement a patch to correct this issue.	2026-07-05	3.3	CVE-2026-14760
radareorg--radare2	A security vulnerability has been detected in radareorg radare2 up to 6.1.6. The affected element is the function r_str_ndup/r_str_append of the file libr/util/str.c. The manipulation leads to integer overflow. An attack has to be approached locally. The exploit has been disclosed publicly and may be used. The identifier of the patch is a20a56917ae85d732e683f8d9078bdcfee92446c. Applying a patch is the recommended action to fix this issue.	2026-07-05	3.3	CVE-2026-14761
ruby--json	Ruby JSON is a JSON implementation for Ruby. Versions 2.9.0 through 2.19.8 are vulnerable to heap buffer overflow when the JSON generator is provided with an oversized streamed object. When streaming to an IO JSON.dump(obj, io) and JSON::State#generate(obj, io) can write past the internal JSON generator buffer when a streamed object contains an attacker-controlled string near 16 KB. Exploitation would result in a reliable process crash/denial of service. This issue has been fixed in version 2.19.9.	2026-06-30	3.7	CVE-2026-54696

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
seaweedfs--seaweedfs	SeaweedFS before 4.30 reflects the callback query parameter verbatim into responses served with Content-Type application/javascript in the shared writeJson helper (weed/server/common.go), with no callback-name validation, no X-Content-Type-Options: nosniff header, and no CORS allow-list. Every JSON endpoint that uses writeJson - including the unauthenticated master endpoints /dir/status, /dir/lookup and /cluster/status, the volume server /status, and the filer directory listing, all reachable in the default configuration (no -whiteList, no security.toml, bound to 0.0.0.0) - can therefore be loaded cross-origin via a script tag with a chosen callback, letting a third-party web page read cluster topology, volume server URLs and gRPC ports, file identifiers, and directory listings. Because the callback string is reflected at the start of the body and no nosniff header is sent, MIME-sniffing clients may also interpret the reflected content as HTML.	2026-06-30	3.1	CVE-2026-58371
seladb--PcapPlusPlus	A vulnerability was found in seladb PcapPlusPlus 25.05. The affected element is the function parse_by_block_type of the file light_pcapng.c of the component LightPcapNg Parser. Performing a manipulation of the argument captured_packet_length results in heap-based buffer overflow. It is possible to initiate the attack remotely. The attack's complexity is rated as high. The exploitability is described as difficult. The exploit has been made public and could be used.	2026-06-29	3.7	CVE-2026-13587
Snowflake--Snowflake CLI	Improper neutralization of local CLI parameters in Snowflake CLI versions prior to 3.19 allowed unintended SQL execution. A user could trigger this issue by supplying crafted values to vulnerable Cortex SQL or object listing command paths, causing Snowflake CLI to execute unintended SQL in the context of that user's Snowflake session. Successful exploitation is constrained to self-injection because the vulnerable parameters were supplied directly through local CLI arguments rather than through project files, repositories, or other external input sources, and impact is limited to the privileges already available to the current session. The fix is available in Snowflake CLI version 3.19, and users must manually upgrade.	2026-06-29	3.6	CVE-2026-13746
SourceCodester--Inventory Management System	A vulnerability was detected in SourceCodester Inventory Management System 1.0. Impacted is an unknown function of the file /api/users_handler.php of the component User Registration Endpoint. Performing a manipulation of the argument full_name results in cross site scripting. The attack is possible to be carried out remotely. The exploit is now public and may be used.	2026-06-29	3.5	CVE-2026-13570
TUBITAK BILGEM Software Technologies Research Institute--Pardus Pen	Improper null termination vulnerability in TUBITAK BILGEM Software Technologies Research Institute Pardus Pen allows Overflow Buffers. This issue affects Pardus Pen: from <=4.1.5 before 4.2.1.	2026-07-05	3.9	CVE-2026-12386
uvnc--UltraVNC	UltraVNC repeater through 1.8.2.2 contains an off-by-one error in the Base64 decode helper used for HTTP Basic authentication. In repeater/webgui/webutils.c:817, the wi_uudecode() function checks whether the input length exceeds the output buffer with a strict greater-than comparison (>), while the correct check should be greater-than-or-equal (>=). When strlen(authdata) equals sizeof(decode), the decoded output length (approximately 3/4 of input) does not overflow the buffer in	2026-07-01	3.7	CVE-2026-44042

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	current practice because the outer HTTP request bounds constrain the Authorization header. However, the defective check leaves a latent off-by-one condition that could become exploitable if the buffering constraints change. The current risk is limited to a one-byte write at the boundary of a 1024-byte stack buffer under constrained conditions.			
WSO2--WSO2 Identity Server	In multi-tenanted deployments, the application consent management mechanism fails to correctly isolate consent scopes between tenants. Consent granted by a user for a specific SaaS application within one tenant can be incorrectly applied to SaaS applications with the same name in other tenants, leading to unintended cross-tenant consent sharing. This vulnerability may result in the exposure of user data across tenants, enabling SaaS applications in different tenants to access and modify information without explicit user authorization. This can lead to unauthorized data access and privacy violations. This vulnerability has no impact if the deployment does not support multi-tenancy.	2026-07-04	3.5	CVE-2025-13475
zcaceres--markdownify-mcp	A weakness has been identified in zcaceres markdownify-mcp up to 1.1.0. The affected element is the function assertPathAllowed of the file src/Markdownify.ts. Executing a manipulation can lead to symlink following. The attack can only be executed locally. The pull request to fix this issue awaits acceptance.	2026-07-05	3.3	CVE-2026-14699
zcaceres--markdownify-mcp	A flaw has been found in zcaceres markdownify-mcp up to 1.1.0. This impacts the function saveToTempFile of the file src/Markdownify.ts of the component webpage-to-markdown/youtube-to-markdown/bing-search-to-markdown. This manipulation causes insufficiently random values. The attack is restricted to local execution. A high degree of complexity is needed for the attack. The exploitability is said to be difficult. The exploit has been published and may be used. The pull request to fix this issue awaits acceptance.	2026-07-05	2.5	CVE-2026-14702
zephyrproject--zephyr	A race condition in the Zephyr Bluetooth Classic RFCOMM host stack (subsys/bluetooth/host/classic/rfcomm.c) mishandles a simultaneous bidirectional session disconnect. When the local device has initiated a session teardown (state BT_RFCOMM_STATE_DISCONNECTING, DISC sent, RTX timer armed) and the connected peer concurrently sends its own DISC frame for dlci 0, rfcomm_handle_disc() invokes rfcomm_session_disconnected(), which unconditionally forced the session to BT_RFCOMM_STATE_DISCONNECTED without ever calling bt_l2cap_chan_disconnect(). Because the recovery timer was also cancelled and a later UA is ignored in the DISCONNECTED state, the session becomes permanently wedged: the underlying L2CAP channel is never released and the session slot in the fixed bt_rfcomm_pool[CONFIG_BT_MAX_CONN] array is never reclaimed (its conn pointer stays set). Subsequent bt_rfcomm_dlc_connect() calls on that connection fail with -EINVAL due to the invalid session state, so RFCOMM service is denied for that peer, and repeated occurrences can exhaust the session pool. The DISC frame is peer-controlled over the air, but exploitation requires the peer's DISC to collide with a local-initiated disconnect (a high-complexity timing race). Impact is availability/resource-leak only; there is no memory-safety, confidentiality, or integrity consequence. The defect shipped in released versions (present in v4.4.0 and earlier). The fix only transitions to DISCONNECTED when the session is	2026-06-30	3.1	CVE-2026-10654

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	not already in DISCONNECTING, preserving the proper L2CAP teardown path.			
zephyrproject--zephyr	Zephyr's DNS resolver detects mDNS (.local) queries in dns_resolve_name_internal() (subsys/net/lib/dns/resolve.c) with memcmp(strrchr(query, '.'), ".local", 7), which always reads a fixed 7 bytes from the suffix pointer. When the resolved hostname's final label is shorter than 7 bytes (e.g. names ending in .org, .com, .net, .io, or a trailing dot), the comparison reads 1-2 bytes past the string's NUL terminator. The hostname (query) is the caller-supplied name passed through the standard getaddrinfo()/dns_get_addr_info()/dns_resolve_name() path and is influenceable by operators or remote inputs (server names from configuration, parsed URLs, or app-facing interfaces). On a tightly-sized buffer with no slack (for example a userspace getaddrinfo call where the hostname is copied with k_usermode_string_alloc_copy to exactly strlen+1 bytes), the over-read crosses the allocation boundary; if that boundary is unmapped (guard page, memory-domain boundary under MPU, or an address sanitizer) the over-read faults, causing a denial of service. The over-read bytes are never returned, so there is no information disclosure. The flaw is compiled only when CONFIG_MDNS_RESOLVER is enabled, exists since v1.10.0, and is fixed by replacing the fixed-length memcmp with a NUL-safe strcmp(ptr, ".local").	2026-07-05	3.7	CVE-2026-10657